ciphertrust.com

November 2004

IronMail® User Manual

Product Version 4.5 SR1

CipherTrust®
Peace of Mind in Messaging™

CipherTrust, Inc.

4800 North Point Parkway

Suite 400

Alpharetta, GA 30022

Phone: (678) 969-9399

©2004 CipherTrust, Inc. CipherTrust and CipherTrust logo are registered trademarks of CipherTrust, Inc. All other company or product names are trademarks or registered trademarks of their respective owners. All rights reserved.

Portions of this product are:

Copyright © 1991-1995 by Stichting Mathematisch Centrum, Amsterdam, The Netherlands. All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies, and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of Stichting Mathematisch Centrum or CWI or Corporation for National Research Initiatives or CNRI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

Copyright © 2001 Sophos. All rights reserved.

Copright © 1989, 1991 Free Software Foundation. All rights reserved.

Copyright © 1997, 1998 Free BSD, Inc. All rights reserved.

Copyright © 1998-2001 Ralf S. Engelschall. All rights reserved.

Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved.

Copyright © 1995-2001 Sun Microsystems, Inc. All rights reserved.

Copyright © 1999-2001 The Apache Software Foundation. All rights reserved.

Copyright © 1995-1998 Eric Young. All rights reserved.

Copyright © 1991-1995 Stichting Mathematisch Centrum, Amsterdam, The Netherlands. All rights reserved.

Copyright © 1998, 1999, 2000, 2001 Martin Roesch. All rights reserved.

Copyright © 1992 Eugene Spafford and Gene Kim. All rights reserved.

Copyright © 1989, 1991, 1992 Carnegie Mellon University. All rights reserved.

Copyright © 2000, 2001 Carnegie Mellon University. All rights reserved.

Copyright © The University of Utah and the Regents of the University of California. All rights reserved.

Copyright © Jason Hunter (jhunter@servlets.com). All rights reserved.

Copyright © 1998-2001 The OpenSSL Project. All rights reserved.

Copyright © 2001 Python Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)."
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL," nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgement: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (htdtp://www.openssl.org)."

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED OR ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptosoft.com). This product includes software written by Tim Hudson (tjh@cryptosoft.com).

Table Of Contents

Introduction **1**
What is IronMail 1

Getting Started **3**
Setting Up IronMail 3
Configuring IronMail 3
Preliminary Information 3
Initial Configuration Wizard 4
Configuring IronMail as a CMC 13
Network Connectivity 16
DNS Configuration 16
Internal Mail Server Configuration 16
Network Firewall Configuration 16

Guarding the Gateway **21**
Gateway Security 21
Controlling the Gateway 21
Gateway Threats 21

Connection Services **23**
Examining Connections 23
The Firewall 23
Mail-Firewall 23
Configuring Mail Services 24
Global Options 25
SMTPI/SMTPIS Services 26
Spoofed Message Protection 31
The SMTPI Service versus the SMTPIS Service over Port 465 32
SMTPO Service 32
Allow Relay 37
Mail Routing 39
Domain-based Routing 39
Edit Domain Routing 41
Add Domain Routing 42
LDAP-based Routing 42
Internal Routing 46

The Virtual Private Network 47
Configure Mail-VPN 47
IMAP4 and POP3 Services 49
Log Level Warning 51
Detecting Intrusions 51
Mail-IDS 51
Application Level Protection 51
Configure Application Level Protection 51
Denial of Service Protection 53
Password Cracking 54
Password Strength 55
Network Level Protection 56
Analysis Console 56
Configure Analysis Console 58
Signature Manager 60
Signature Updates 61
Protection at the System Level 62
Program Integrity 62
Filesystem Integrity 62
Anomaly Detection 63
Configure Anomaly Detection 63
Create Anomaly Rules 65
Show Anomaly Rules 68
ADE Rules 69
Connection Control 70
Vulnerability Assessment 71

Browser-Based Mail 73

Secure WebMail 73
HTTP Proxy 73
Configure Secure WebMail 73
HTTP Routing 76
Host-Based Routing 77
Path-Based Routing 80
Portal Page Routing 83
IronWebMail Portal Login 86
Secondary Authentication 88

Custom IWM Page 89
Signature Configuration 89
Strong Client Authentication 90
Installing Public Keys 91

Message Services 93

Examining Messages 93
IronMail's Queues 93
Introducing the Queues 93
Inside the SuperQueue 98
SuperQueue Functions 99
Managing Policy 103
Policy Manager 103
Creating IronMail Policy 104
Queue Whitelisting 104
Address Masquerade 113
Managing Groups 115
Monitoring Mail 121
Encrypted Messages 135
Off-Hour Delivery 146
Filtering Message Attachments 148
Filtering Message Content 167
Stamping Messages 191
Mail Notification 198
End User Quarantine 201
End User Whitelists 215
Virus Protection 222
Anti-Virus 222
Configure Anti-Virus 222
Extension Override 223
Current Anti-Virus Information 225
Auto Anti-Virus Updates 227
Manual Anti-Virus Updates 228
Log File for Anti-Virus File Updating 230
Capturing Spam 230
Anti-Spam Overview 230
General Anti-Spam Strategy 231

Denying Mail 234
Reverse DNS 238
Blackhole Lists 241
Statistical Detection 247
Analyzing Headers 252
Sender Policy Framework 269
Bayesian Filtering 271
Profiling Spam 274
Reporting Spam 288
Queue Manager 294
Queue Information 294
Configure Queues 301
Setting the Queue Order 307
Outbound Messages 309
Searches 315
Domain Priority 330
Quarantine Types 333
Refreshing the Queue Information Data 335
Using the Quarantine Queue 335
Consolidated Quarantine Server 336

Secure Communication 337

Overview 337
IronMail Security Strategy 337
Managing Certificates 338
Certificate Manager 338
Generate CSR 338
Types of Certificates 341
Installing X.509 Certificates 342
Storing Certificates 343
Exporting Certificates 345
Importing Certificates 347
Configuring Mail Certificates 350
Secure Delivery 350
Secure Delivery 350
Boundary to Boundary 351
SSL 351

S/MIME 354
External S/MIME 354
Internal S/MIME 357
PGP 358
External PGP Key 358
Internal PGP 360
Secure Web Delivery 362
SWD Overview 362
Configure Router 363
Secure Web Delivery Server 363
Configure Secure Web Delivery 363
Configure Server 365
User List 366
Customizing SWD Pages 370
Checking Logs 371

IronMail Administration 373

Reporting and Monitoring 373
Health Monitor 373
Health Monitor Tests and Alerts 378
DNS Hijack Protection 379
IronMail Alerts 382
Alert Levels 382
Alert Manager 382
Alert Class 383
Alert Mechanism 388
Alert Viewer 392
Table of IronMail-generated Alerts 394
Dropped Email Alerts 411
Importing MIBs 411
Reporting and Logging 412
Reports and Log Files 412
IronMail Reports 412
IronMail Logs 438
Cleanup Schedule 463
Configure Mail Certificates 465
Web Administration 466

User Accounts 466
Allowed IPs 468
Configure 470
Known Browser Issues 471
Change Password 471

System Functions 473

Configuring the System 473
Configuration 473
IronMail 473
Out-of-Band Management 476
Routing 478
The Serial Port 479
SSH Configuration 480
Backup 482
Restore 485
Check Tool 487
UPS Statistics 488
Power Down and Restart 489
Date and Time 489
Daylight Savings Time 491
System Updates 491
Software Updates 491
Virus Updates 493
Threat Response Updates 495
Mail-IDS Updates 496
Configure Auto-Updates 497
License Manager 498
Store CMC Key 499
Resetting Keys 501

The Command Line 503

Command Line Interface 503
The Commands 503
Command Overview 503
The HELP Command 505
The EDIT Command 505

The RUN Command 506
The SET Command 507
The SHOW Command 509
The SYSTEM Command 514
The TAIL Command 515
The TEST Command 515

Watching the System 517
Monitoring Conditions 517
Opening Graphs 517
Graphical Analysis 517
Reporting Utilization 517
Queue Graphs 519
Queue Load Statistics 519
Queue Process Statistics 520
Queue Action Statistics 521
System Graphs 521
CPU Utilization: 522
Memory Utilization 523
Disk Input/Output Utilization 523
File System Utilization 524
Network Utilization 524
Statistical Analysis 525
The Dashboard 525

Customizing Pages 529
Customizing IronMail Pages 529
Customizable Pages 529
Customizing SWD 529
Customizing IWM 534
Customizing EUQ 536
Cascading Stylesheets 537
Performing Customizations 541
Modifying the HTML Template 542

Appendices 545
Appendix 1: Formatting Requirements for Importing Lists into IronMail version 4.5 545
Appendix 2: Daily Policy Compliance Report - Summary and Statistics : 01/28/2004 551

Appendix 3: Configuring IronWebMail for MS Exchange 559
Appendix 4: What is LDAP? 563
Appendix 5: Tips and Guidelines 565
Special Characters in Email Addresses 565
File Types From Which IronMail Can Extract Content 565
Appendix 6: Vulnerability Assessment Report 567
Document History: 573
Index 575

INTRODUCTION

What is IronMail

"Email" has grown over the years from a simple, personal messaging system to a complex business tool. However, along with email's growth in functionality came an increase in related problems. Viruses, hackers, Spam, and imprudent email usage are just a few examples. While the marketplace has produced a variety of software solutions to address these issues, they have for the most part focused on a single email problem (e.g., only virus protection, or only content filtering). To date, only one or two products besides IronMail® have attempted to address the entire gamut of email security. However, the problem with the other "comprehensive" packages is that despite the security solutions they offer, they are not, themselves, protected from hackers and email threats. And that's the IronMail difference. All of IronMail's functionality (virus protection, spam blocking, content filtering, email *policy* enforcement, VPN, webmail, etc.) is protected behind a hardened application and operating system, and monitored with state-of-the-art hacker-detection systems that can automatically drop offensive connections and alert the mail and/or security administrator if an attack on the appliance is detected.

CipherTrust, the developer of IronMail, is laser-focused on providing comprehensive security and stopping every possible attack that might compromise your email infrastructure.

Today's enterprise faces at least five potential threats to its e-mail *network*:

- Spam, including phishing, spoofing, and sheer volume attacks;
- Viruses;
- Denial of Service attacks;
- Intrusions; and
- Webmail Attacks.

These threats can represent an enormous financial drain and cost businesses real money. IronMail is designed to protect the network against them all.

GETTING STARTED

Setting Up IronMail

The initial setup for IronMail includes at least two major components, and possibly a third. The Installer or Administrator must set up the basic IronMail appliance to allow its further configuration after the basic initialization is completed; they must also perform essential setup for connectivity to the internet and to the mail *network*. The third component is necessary only if the IronMail appliance is being set up as a Centralized Management Console (*CMC*).

Setup results in only the most basic configuration of IronMail. Once all initial setup is complete, the Administrator will perform the detailed configuration that prepares IronMail to protect the specific network.

Configuring IronMail

Preliminary Information

IronMail—whether intended as a stand-alone appliance or as a Centralized Management Console—uses a simple wizard to set the initial values required for it to become minimally functional. Before you run the wizard, obtain the information requested in the form below. Your network administrator should be able to assist you in determining the network information. (A copy of this Information Gathering Form appears at the back of the Setup Guide so it may be removed for easy information gathering.)

1. Have on hand the License Key that was emailed to you for the IronMail appliance. The License Key contains information that determines whether this appliance is a *Centralized Management Console* for enterprise environments or a stand-alone IronMail.
2. Create a *host name* for this appliance.
3. Determine the *domain name* to which this appliance belongs.
4. Assign an *IP address* for this appliance.
5. Determine the *Subnet* Mask for this appliance.
6. Specify the Default Router the appliance will use.
7. Specify the IP Address of at least one of your DNS Servers (This appliance must be able to connect to it.)
8. Provide the fully qualified domain names of up to three Network Time *Protocol* servers. (IronMail identifies three servers by default.)
9. Specify the appliance's time zone by selecting from the pick list the city nearest the appliance. (The selected city must be in the same time zone as IronMail.)
10. For "stand-alone" IronMail only! — Specify the fully qualified domain name of your default mail server. (If you have dedicated servers handling incoming and outgoing mail, or other services, select one to enter during the wizard setup—the remaining servers will be configured later.) This information is not necessary for configuring a Centralized Management Console.
11. Specify the IP address of the default mail server you identified above.
12. Specify your default email domain.
13. Determine if you want IronMail to use secure *POP3* or IMAP 4 with your internal server. (Your internal server must have a Security Certificate installed on it for secure POP3 or *IMAP4* to be implemented.).

Verify this information with your Network Administrator prior to running the appliance's Initial Configuration Wizard.

Initial Configuration Wizard

IronMail ships with a pre-installed, albeit unsigned, Security Certificate. IronMail only allows administrative sessions with it over a secure *SSL* (https) connection, for which a Security Certificate is required. The default Security Certificate is adequate for creating these secure connections from your browser to the IronMail appliance, but is not adequate for providing SSL security for your email infrastructure. Until you install a valid Security Certificate from a Certificate Authority, your browser will display a Security Alert each time you logon to the appliance. Clicking **Yes** at the prompt allows you to proceed.

You must connect to the appliance to enter some preliminary values in an Initial Configuration Wizard in order to make the appliance initially functional. Use a client workstation (any Windows PC) as IronMail's "front end." There are two ways you can connect to the appliance:

- Use a network "cross-over" cable to physically connect a PC workstation to IronMail. (The cable plugs into the network port on each device.)
- Install IronMail in your existing network, but set a PC workstation's netmask to match IronMail's default *IP address* and netmask.

For either type of connection, the client workstation must temporarily change its IP address and netmask to match IronMail's default values (IP Address: **192.168.0.254**, Netmask: **255.255.255.0**). That is, change your workstation IP address to 192.168.0.xxx, and the netmask to 255.255.255.0 (where xxx is any number between 0-253).

1. Launch Internet Explorer on the client workstation and navigate to IronMail's built-in default IP address:

   https://192.168.0.254

   You must add the letter "s" after "http."

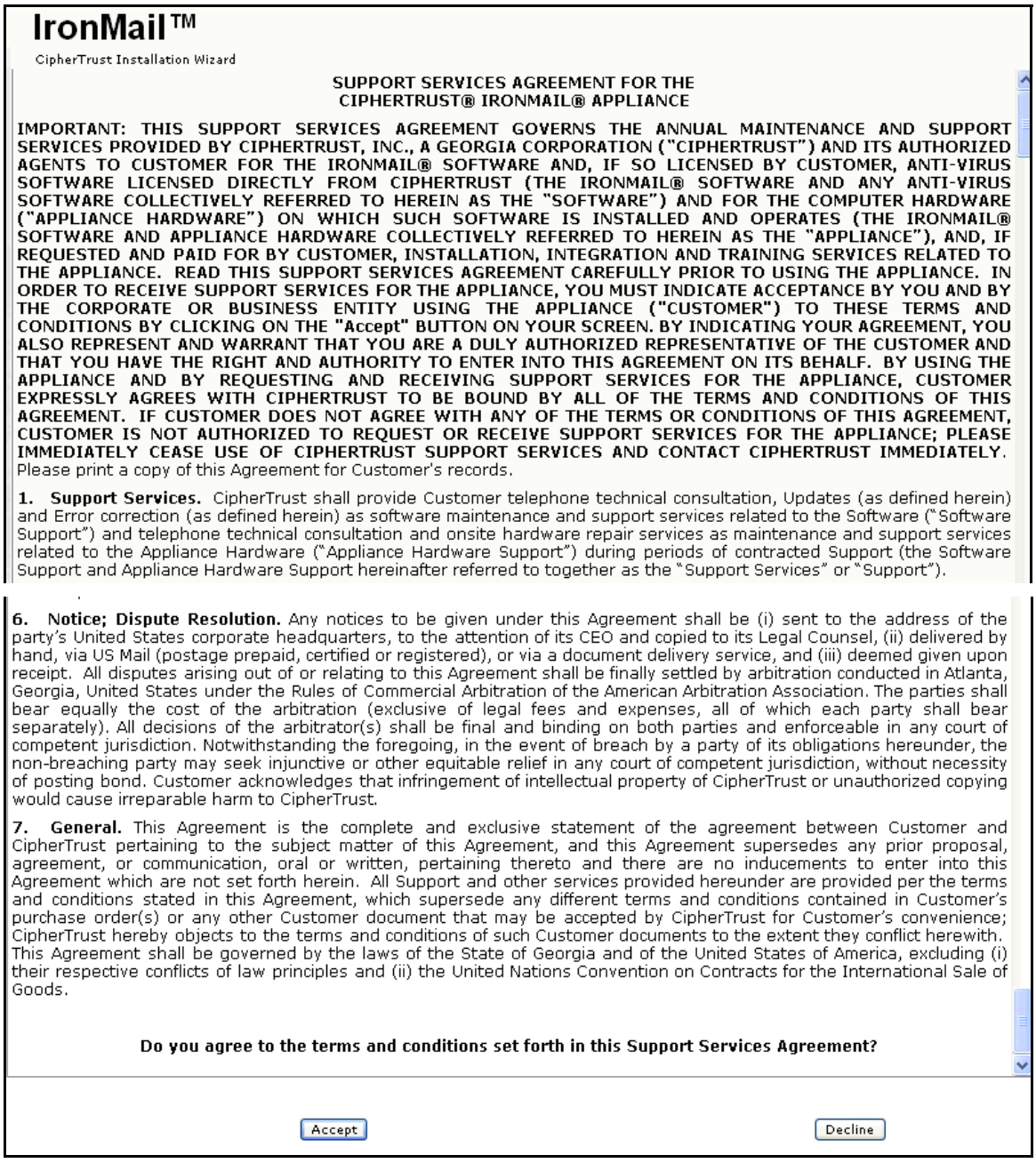
   The opening screen for the Installation Wizard displays. Click **Next** to begin the installation process.

CipherTrust
ENTERPRISE EMAIL SECURITY
IronMail™
CipherTrust Installation Wizard
This wizard will take you step-by-step through the network configuration of the IronMail.. Once you have entered all the information, the system will reboot and the Web Administration will be accessible.
Next

2. The first screen to appear is the Master Sale and License Agreement. After you have read the agreement, click **Accept** or **Decline**. If you choose to Decline, the installation wizard will close and the appliance will not run. If you choose Accept, the wizard proceeds to the next step.

IronMail™
CipherTrust Installation Wizard
MASTER SALE AND LICENSE AGREEMENT FOR THE CIPHERTRUST® IRONMAIL® APPLIANCE
IMPORTANT: THIS MASTER SALE AND LICENSE AGREEMENT GOVERNS USE OF THE IRONMAIL® SOFTWARE AND, IF LICENSED IN ADDITION TO THE IRONMAIL® SOFTWARE, THE ANTI-VIRUS SOFTWARE (THE IRONMAIL® SOFTWARE AND, IF APPLICABLE, THE ANTI-VIRUS SOFTWARE COLLECTIVELY REFERRED TO AS THE "SOFTWARE") ON THE APPLIANCE HARDWARE ON WHICH THE SOFTWARE IS INSTALLED AND OPERATES (THE IRONMAIL® SOFTWARE AND APPLIANCE HARDWARE BEING REFERRED TO HEREIN TOGETHER AS THE "APPLIANCE"). READ THIS MASTER SALE AND LICENSE AGREEMENT CAREFULLY PRIOR TO USING THE APPLIANCE. IN ORDER TO USE THIS APPLIANCE, YOU MUST INDICATE ACCEPTANCE BY YOU AND BY THE CORPORATE OR BUSINESS ENTITY WHICH IS USING THE APPLIANCE ("CUSTOMER") TO THESE TERMS AND CONDITIONS BY CLICKING ON THE "Accept" BUTTON ON YOUR SCREEN. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE CUSTOMER AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON ITS BEHALF. BY USING THE APPLIANCE, CUSTOMER EXPRESSLY AGREES WITH CIPHERTRUST, INC., A GEORGIA CORPORATION ("CIPHERTRUST"), TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT, CUSTOMER IS NOT AUTHORIZED TO USE THE APPLIANCE FOR ANY PURPOSE WHATSOEVER; PLEASE IMMEDIATELY CEASE USE AND CONTACT CIPHERTRUST. Please print a copy of this Agreement for Customer's records.
1. License. This Agreement grants Customer (i) a non-exclusive, non-transferable license to use one copy of the IronMail® Software (the "IronMail® License"), and, if purchased by Customer, (ii) a non-exclusive, non-transferable license to use one copy of the anti-virus software for a specific period of time as indicated on the Customer's purchase order and/or CipherTrust's invoice (the "Anti-Virus License") (the IronMail® License and, if applicable, Anti-Virus License collectively referred to as the "License") solely on and in conjunction with the Appliance Hardware on which it is installed. This Agreement also authorizes Customer to use the related written materials and "online" or electronic documentation (collectively, "Documentation") solely in conjunction with the Appliance. CipherTrust and its suppliers retain title to all patents, copyrights, trade secrets, trademarks and other intellectual property rights in the Software and the Documentation. This Agreement shall not affect a sale of the Software, and Customer shall not acquire hereunder any
Customer from its possession and use of the Appliance during the Evaluation shall be treated as confidential per the terms of Section 14 herein. Upon Customer's payment for the Appliance and the license fee for the Software, the temporary License granted per this Section shall automatically become perpetual (subject to Section 2 herein). In the event Customer decides not to purchase the Appliance and a license for the Software, the temporary License granted per this Section will be automatically revoked at the end of the Evaluation Period, and Customer at its expense shall promptly return the Appliance to CipherTrust, properly packaged for commercial shipment to ensure no physical damage during transit; Customer will be invoiced by CipherTrust for an amount equal to the replacement cost of the Appliance should the returned Appliance be delivered to CipherTrust damaged due to insufficient and improper packaging by Customer. Upon Customer's failure to timely return the Appliance per the foregoing sentence, CipherTrust shall issue an invoice to Customer for the purchase at list price of the Appliance and a Software license under the terms of this Agreement. The terms of this Section shall apply only (i) to Customer's use and possession of the Appliance for Evaluation purposes and (ii) in the absence of a written evaluation agreement signed by both parties, which if executed shall prevail and control during the Evaluation Period. The terms stated in Sections 2, 5 and 16 of this Agreement shall not apply during the Evaluation Period.
18. General. This Agreement is the complete and exclusive statement of the agreement between Customer and CipherTrust concerning the subject matter covered hereby, this Agreement supersedes any prior proposal, agreement, or communication, oral or written, pertaining to the such subject matter and there are no inducements to enter into this Agreement which are not set forth herein. All products and services provided hereunder are provided per the terms and conditions stated in this Agreement, which supersede any different terms and conditions contained in Customer's purchase order(s) or any other Customer document that may be accepted by CipherTrust for Customer's convenience; CipherTrust hereby objects to the terms and conditions of such Customer documents to the extent they conflict herewith. This Agreement shall be governed by the laws of the State of Georgia and of the United States of America, excluding (i) their respective conflicts of law principles and (ii) the United Nations Convention on Contracts for the International Sale of Goods.
Do you agree to the terms and conditions set forth in this Master Sale and License Agreement?
Accept
Decline

3. The next screen that opens displays the Support Services Agreement. After you have read the agreement, click **Accept** or **Decline**. If you choose to Decline, the installation wizard will close and the appliance will not run. If you choose Accept, the wizard proceeds to the next step.

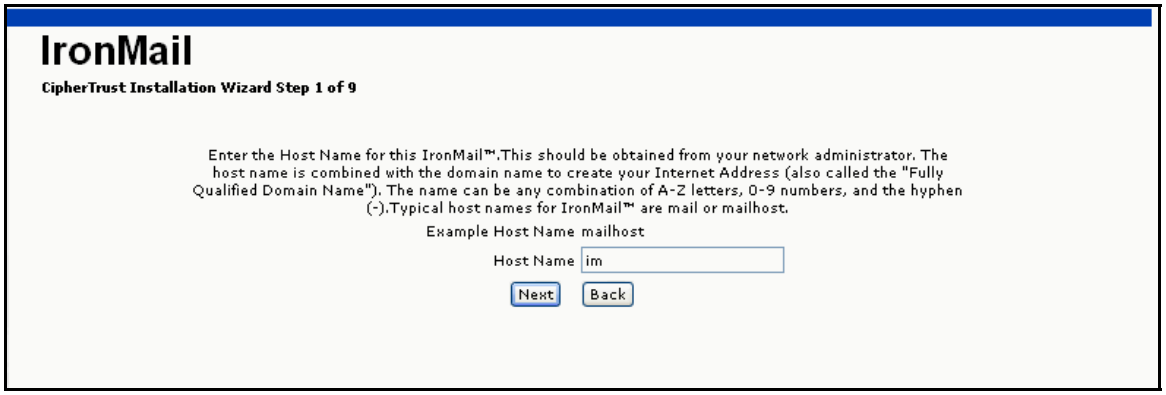

IronMail™
CipherTrust Installation Wizard
SUPPORT SERVICES AGREEMENT FOR THE
CIPHERTRUST® IRONMAIL® APPLIANCE
IMPORTANT: THIS SUPPORT SERVICES AGREEMENT GOVERNS THE ANNUAL MAINTENANCE AND SUPPORT SERVICES PROVIDED BY CIPHERTRUST, INC., A GEORGIA CORPORATION ("CIPHERTRUST") AND ITS AUTHORIZED AGENTS TO CUSTOMER FOR THE IRONMAIL® SOFTWARE AND, IF SO LICENSED BY CUSTOMER, ANTI-VIRUS SOFTWARE LICENSED DIRECTLY FROM CIPHERTRUST (THE IRONMAIL® SOFTWARE AND ANY ANTI-VIRUS SOFTWARE COLLECTIVELY REFERRED TO HEREIN AS THE "SOFTWARE") AND FOR THE COMPUTER HARDWARE ("APPLIANCE HARDWARE") ON WHICH SUCH SOFTWARE IS INSTALLED AND OPERATES (THE IRONMAIL® SOFTWARE AND APPLIANCE HARDWARE COLLECTIVELY REFERRED TO HEREIN AS THE "APPLIANCE"), AND, IF REQUESTED AND PAID FOR BY CUSTOMER, INSTALLATION, INTEGRATION AND TRAINING SERVICES RELATED TO THE APPLIANCE. READ THIS SUPPORT SERVICES AGREEMENT CAREFULLY PRIOR TO USING THE APPLIANCE. IN ORDER TO RECEIVE SUPPORT SERVICES FOR THE APPLIANCE, YOU MUST INDICATE ACCEPTANCE BY YOU AND BY THE CORPORATE OR BUSINESS ENTITY USING THE APPLIANCE ("CUSTOMER") TO THESE TERMS AND CONDITIONS BY CLICKING ON THE "Accept" BUTTON ON YOUR SCREEN. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE CUSTOMER AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON ITS BEHALF. BY USING THE APPLIANCE AND BY REQUESTING AND RECEIVING SUPPORT SERVICES FOR THE APPLIANCE, CUSTOMER EXPRESSLY AGREES WITH CIPHERTRUST TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT, CUSTOMER IS NOT AUTHORIZED TO REQUEST OR RECEIVE SUPPORT SERVICES FOR THE APPLIANCE; PLEASE IMMEDIATELY CEASE USE OF CIPHERTRUST SUPPORT SERVICES AND CONTACT CIPHERTRUST IMMEDIATELY.
Please print a copy of this Agreement for Customer's records.
1. Support Services. CipherTrust shall provide Customer telephone technical consultation, Updates (as defined herein) and Error correction (as defined herein) as software maintenance and support services related to the Software ("Software Support") and telephone technical consultation and onsite hardware repair services as maintenance and support services related to the Appliance Hardware ("Appliance Hardware Support") during periods of contracted Support (the Software Support and Appliance Hardware Support hereinafter referred to together as the "Support Services" or "Support").
6. Notice; Dispute Resolution. Any notices to be given under this Agreement shall be (i) sent to the address of the party's United States corporate headquarters, to the attention of its CEO and copied to its Legal Counsel, (ii) delivered by hand, via US Mail (postage prepaid, certified or registered), or via a document delivery service, and (iii) deemed given upon receipt. All disputes arising out of or relating to this Agreement shall be finally settled by arbitration conducted in Atlanta, Georgia, United States under the Rules of Commercial Arbitration of the American Arbitration Association. The parties shall bear equally the cost of the arbitration (exclusive of legal fees and expenses, all of which each party shall bear separately). All decisions of the arbitrator(s) shall be final and binding on both parties and enforceable in any court of competent jurisdiction. Notwithstanding the foregoing, in the event of breach by a party of its obligations hereunder, the non-breaching party may seek injunctive or other equitable relief in any court of competent jurisdiction, without necessity of posting bond. Customer acknowledges that infringement of intellectual property of CipherTrust or unauthorized copying would cause irreparable harm to CipherTrust.
7. General. This Agreement is the complete and exclusive statement of the agreement between Customer and CipherTrust pertaining to the subject matter of this Agreement, and this Agreement supersedes any prior proposal, agreement, or communication, oral or written, pertaining thereto and there are no inducements to enter into this Agreement which are not set forth herein. All Support and other services provided hereunder are provided per the terms and conditions stated in this Agreement, which supersede any different terms and conditions contained in Customer's purchase order(s) or any other Customer document that may be accepted by CipherTrust for Customer's convenience; CipherTrust hereby objects to the terms and conditions of such Customer documents to the extent they conflict herewith. This Agreement shall be governed by the laws of the State of Georgia and of the United States of America, excluding (i) their respective conflicts of law principles and (ii) the United Nations Convention on Contracts for the International Sale of Goods.
Do you agree to the terms and conditions set forth in this Support Services Agreement?
Accept
Decline

4. Copy the text file containing the License Key for the appliance, and paste the key into the input field on the next screen.

You must include all of the beginning and ending lines that appear with the License Key, as shown: "======Begin CipherTrust License======" and "======End CipherTrust License======."

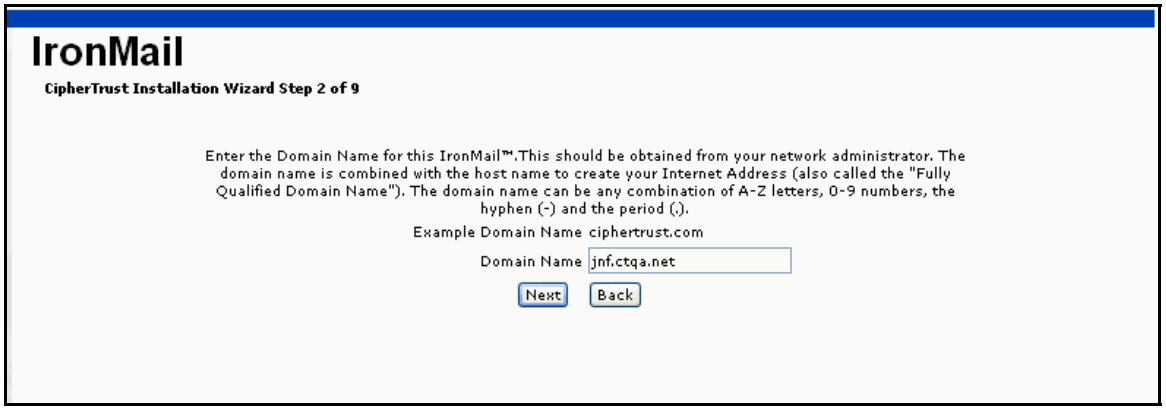
After pasting in the key, click **Next**.

5. Enter the *host name* for the appliance, created by your Network Administrator. The host name is the text preceding the *domain name*. In the example "servername.yourdomain.com" "servername" is the *host name*, and "yourdomain.com" is the domain name.


IronMail
CipherTrust Installation Wizard Step 1 of 9
Enter the Host Name for this IronMail™.This should be obtained from your network administrator. The host name is combined with the domain name to create your Internet Address (also called the "Fully Qualified Domain Name"). The name can be any combination of A-Z letters, 0-9 numbers, and the hyphen (-).Typical host names for IronMail™ are mail or mailhost.
Example Host Name mailhost
Host Name im
Next
Back

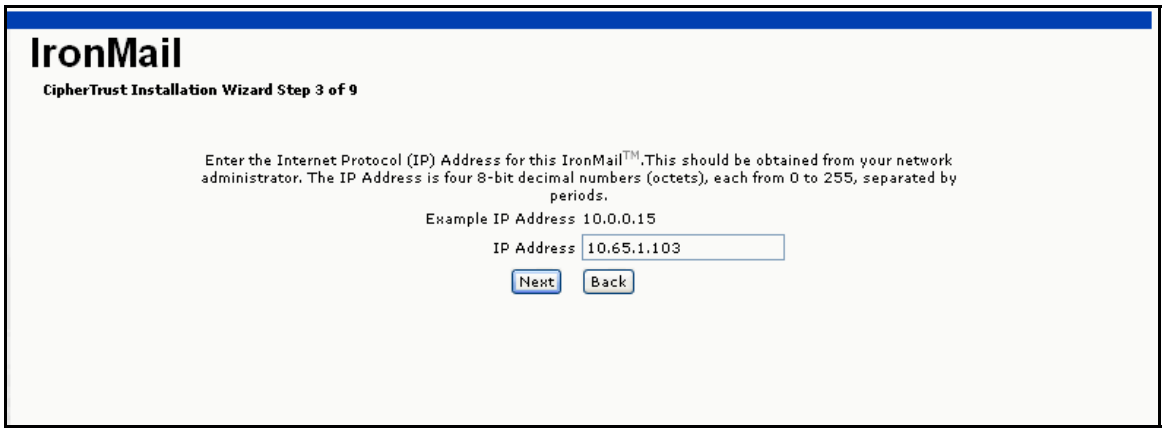
Click **Next**.

6. Enter the domain name for the domain to which the appliance will belong (e.g., "yourdomain.com").


IronMail
CipherTrust Installation Wizard Step 2 of 9
Enter the Domain Name for this IronMail™.This should be obtained from your network administrator. The domain name is combined with the host name to create your Internet Address (also called the "Fully Qualified Domain Name"). The domain name can be any combination of A-Z letters, 0-9 numbers, the hyphen (-) and the period (.).
Example Domain Name ciphertrust.com
Domain Name jnf.ctqa.net
Next
Back

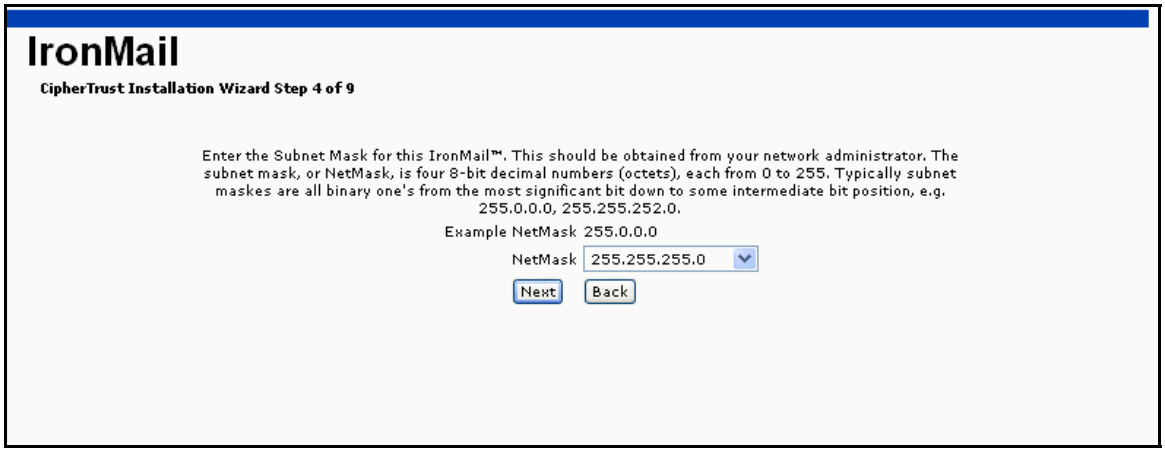
Click **Next**.

7. Enter the IP address assigned by your Network Administrator for this appliance.


IronMail
CipherTrust Installation Wizard Step 3 of 9
Enter the Internet Protocol (IP) Address for this IronMail™.This should be obtained from your network administrator. The IP Address is four 8-bit decimal numbers (octets), each from 0 to 255, separated by periods.
Example IP Address 10.0.0.15
IP Address 10.65.1.103
Next
Back

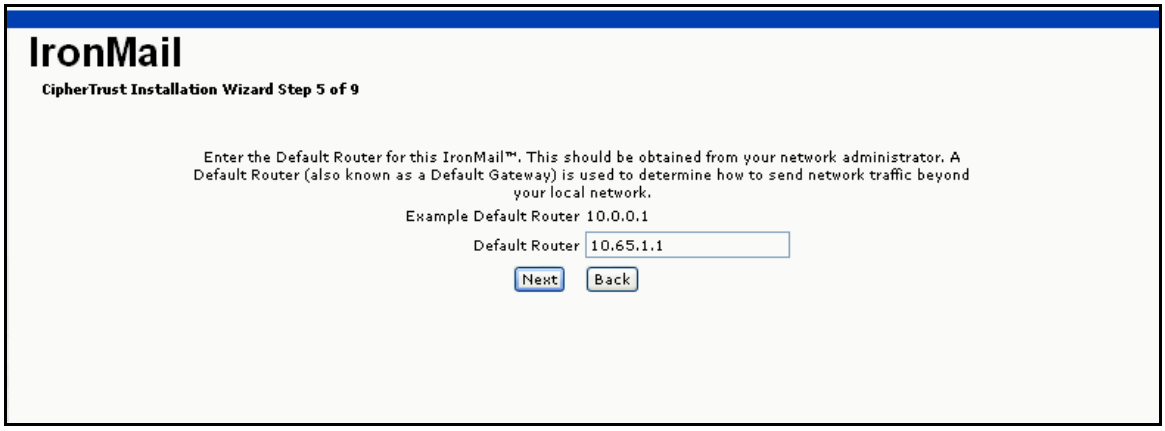
Click **Next**.

8. Enter the *subnet* mask for this IronMail, as provided by your Network Administrator.


IronMail
CipherTrust Installation Wizard Step 4 of 9
Enter the Subnet Mask for this IronMail™. This should be obtained from your network administrator. The subnet mask, or NetMask, is four 8-bit decimal numbers (octets), each from 0 to 255. Typically subnet maskes are all binary one's from the most significant bit down to some intermediate bit position, e.g. 255.0.0.0, 255.255.252.0.
Example NetMask 255.0.0.0
NetMask 255.255.255.0
Next
Back

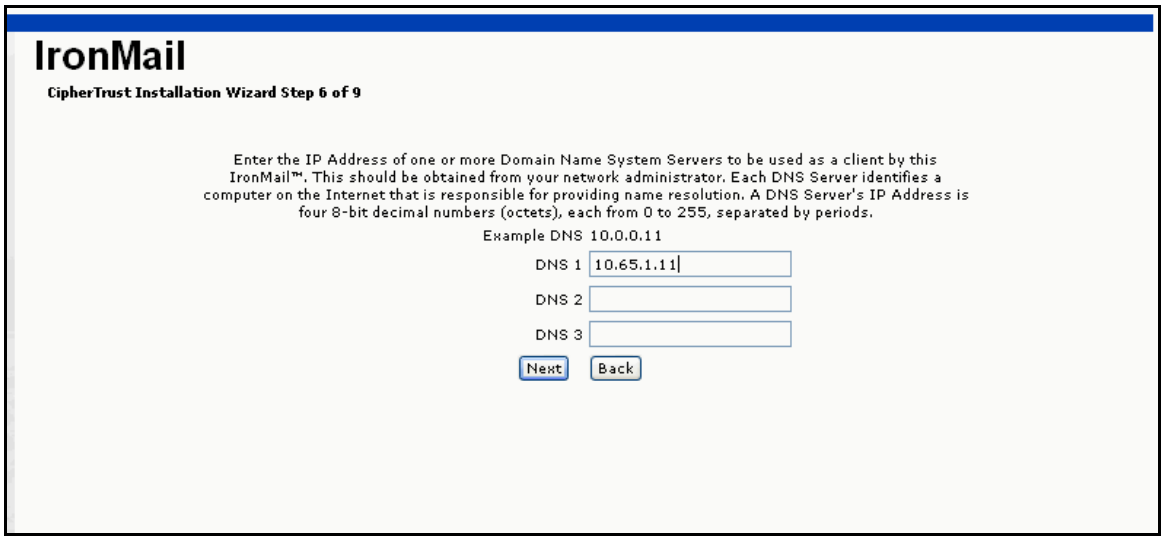
Click **Next**.

9. Enter the IP address for the Default Router for this appliance. The router address is provided by the Network Administrator.


IronMail
CipherTrust Installation Wizard Step 5 of 9
Enter the Default Router for this IronMail™. This should be obtained from your network administrator. A Default Router (also known as a Default Gateway) is used to determine how to send network traffic beyond your local network.
Example Default Router 10.0.0.1
Default Router 10.65.1.1
Next
Back

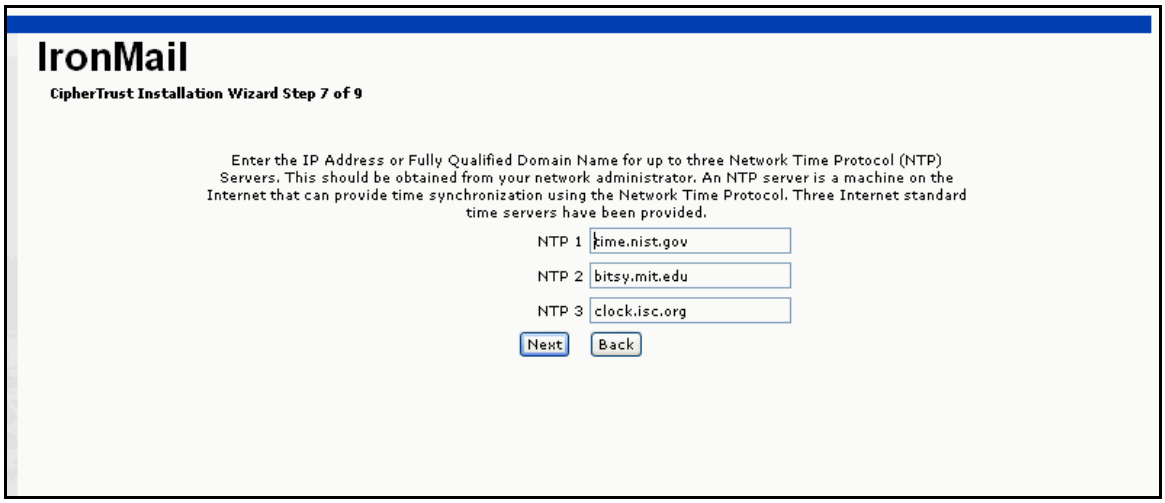
Click **Next**.

10. Enter the IP address for at least one of your DNS Servers (you may have up to three). The *DNS server* will be used as a client for this IronMail.


IronMail
CipherTrust Installation Wizard Step 6 of 9
Enter the IP Address of one or more Domain Name System Servers to be used as a client by this IronMail™. This should be obtained from your network administrator. Each DNS Server identifies a computer on the Internet that is responsible for providing name resolution. A DNS Server's IP Address is four 8-bit decimal numbers (octets), each from 0 to 255, separated by periods.
Example DNS 10.0.0.11
DNS 1 10.65.1.11
DNS 2
DNS 3
Next
Back

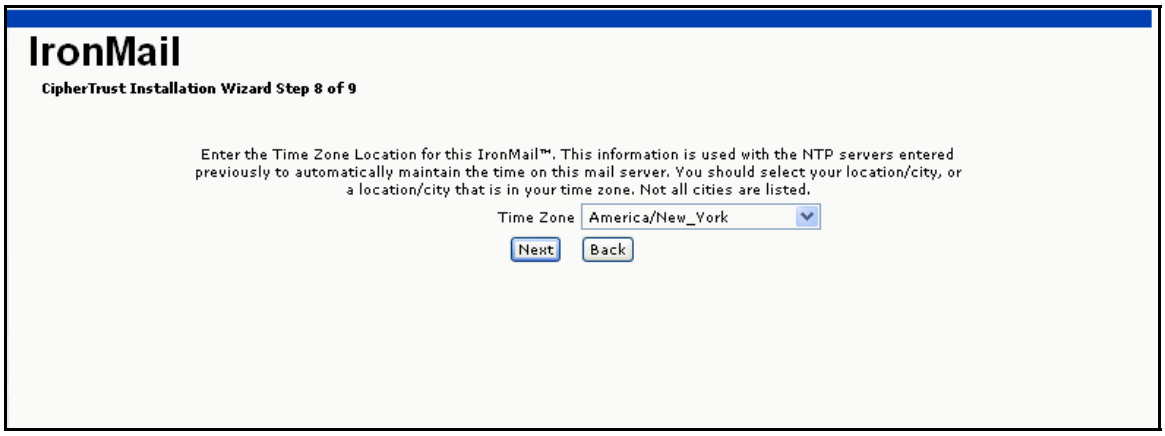
Click **Next**.

11. Enter the IP address or the fully qualified domain name for up to three Network Time *Protocol* (NTP) servers, as provided by the Network Administrator.


IronMail
CipherTrust Installation Wizard Step 7 of 9
Enter the IP Address or Fully Qualified Domain Name for up to three Network Time Protocol (NTP) Servers. This should be obtained from your network administrator. An NTP server is a machine on the Internet that can provide time synchronization using the Network Time Protocol. Three Internet standard time servers have been provided.
NTP 1 time.nist.gov
NTP 2 bitsy.mit.edu
NTP 3 clock.isc.org
Next
Back

Click **Next**.

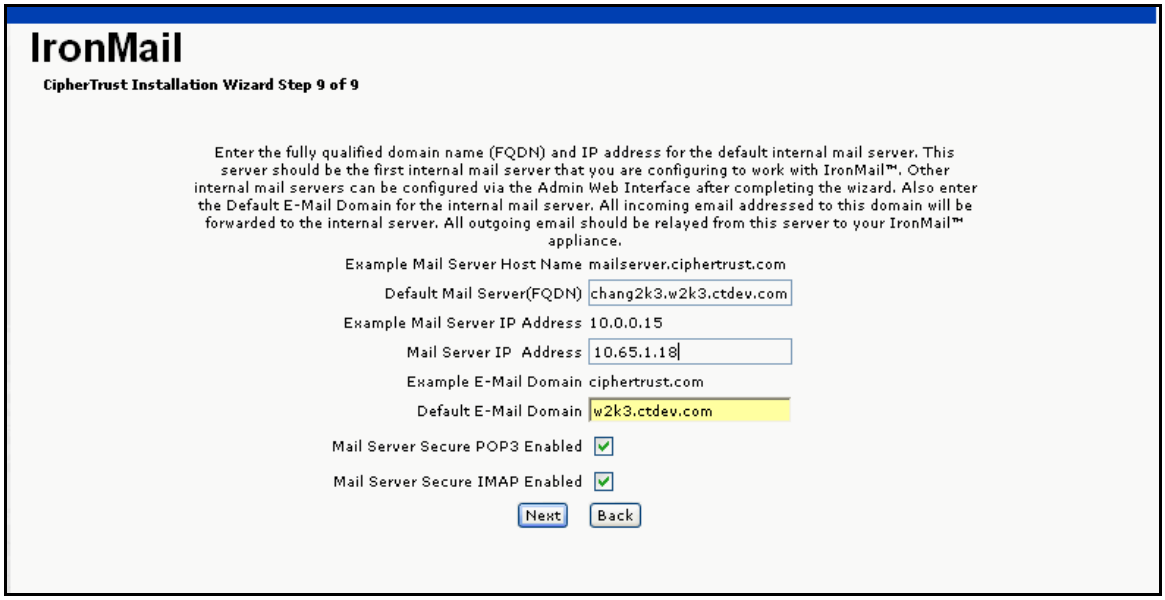
12. Specify the appliance's time zone by selecting from the pick list your own location or city, or a location/city that is in the same time zone.


IronMail
CipherTrust Installation Wizard Step 8 of 9
Enter the Time Zone Location for this IronMail™. This information is used with the NTP servers entered previously to automatically maintain the time on this mail server. You should select your location/city, or a location/city that is in your time zone. Not all cities are listed.
Time Zone
America/New_York
Next
Back

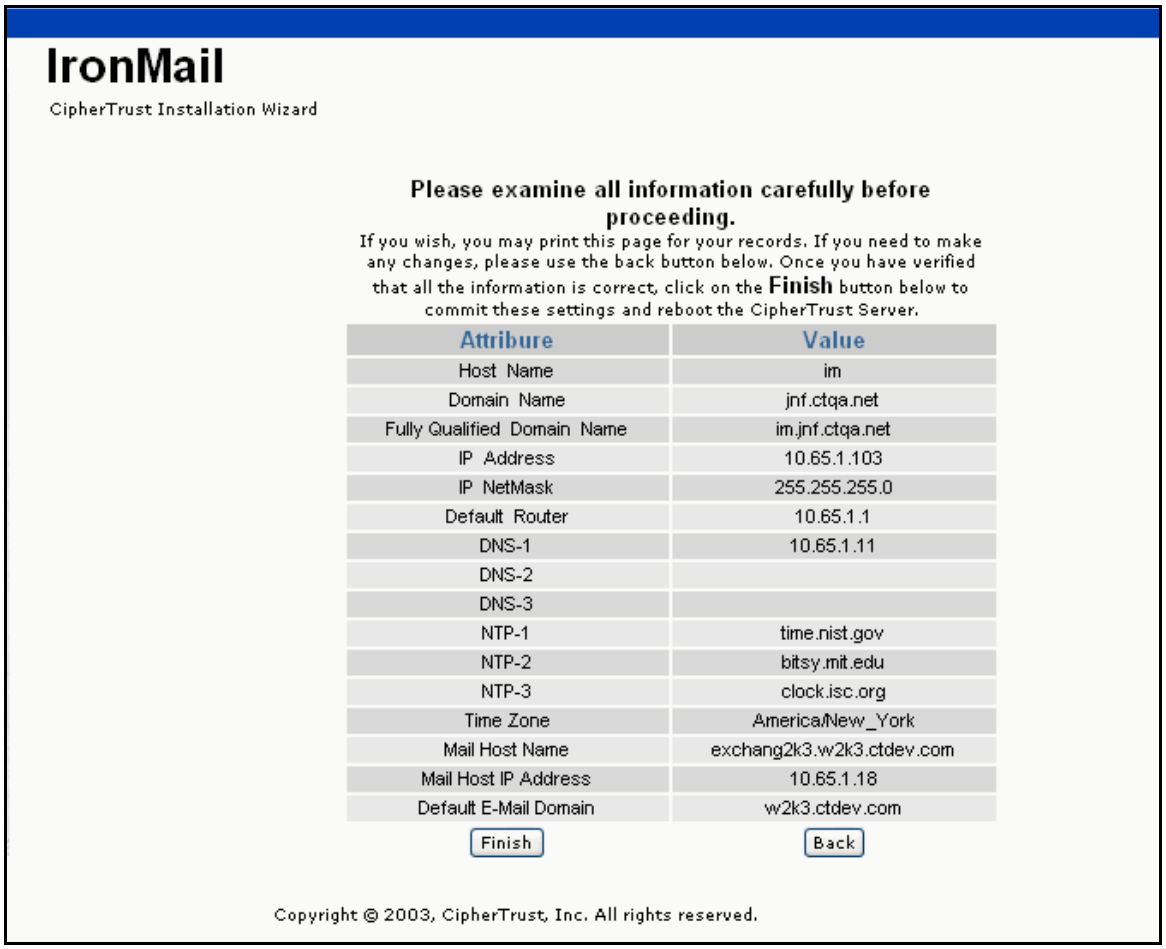
Click **Next**.

13. If you are configuring ***a stand-alone IronMail appliance***, you must enter information about your default email server. If you have more than one email server, enter only the information about the default server. You can configure additional servers after you complete the Installation Wizard.

    If you are configuring ***a Centralized Management Console***, you do not have to provide information about internal mail servers. Skip this step by clicking **Next**, and proceed to verifying your information.


IronMail
CipherTrust Installation Wizard Step 9 of 9
Enter the fully qualified domain name (FQDN) and IP address for the default internal mail server. This server should be the first internal mail server that you are configuring to work with IronMail™. Other internal mail servers can be configured via the Admin Web Interface after completing the wizard. Also enter the Default E-Mail Domain for the internal mail server. All incoming email addressed to this domain will be forwarded to the internal server. All outgoing email should be relayed from this server to your IronMail™ appliance.
Example Mail Server Host Name mailserver.ciphertrust.com
Default Mail Server(FQDN) chang2k3.w2k3.ctdev.com
Example Mail Server IP Address 10.0.0.15
Mail Server IP Address 10.65.1.18
Example E-Mail Domain ciphertrust.com
Default E-Mail Domain w2k3.ctdev.com
Mail Server Secure POP3 Enabled
Mail Server Secure IMAP Enabled
Next
Back

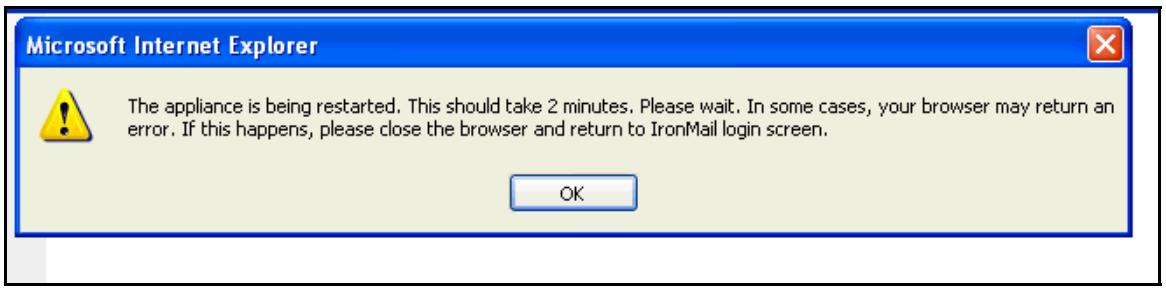
14. Verify that the information you have provided is correct. You can use the Back buttons to return to previous steps and make corrections, should you detect errors. You may want to print this screen for your records once you have verified the information.



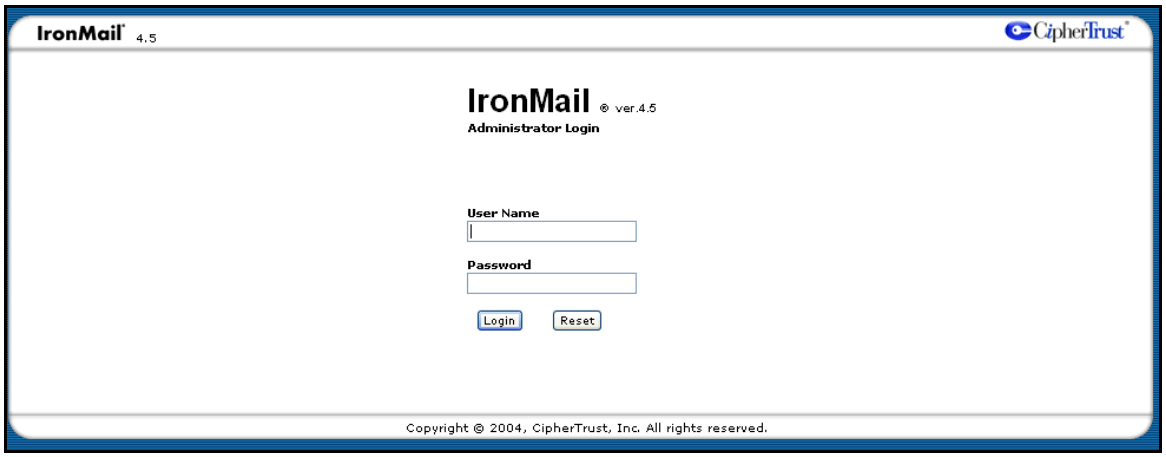
If you inadvertently enter the IP address incorrectly and fail to print this page showing the appliance's dot-decimal number, you will be unable to log onto IronMail when you later browse to what you thought was the correct address. Log onto IronMail via attached keyboard and command line interface to reset the appliance to its default factory settings.

Click **Finish** after the information has been verified.

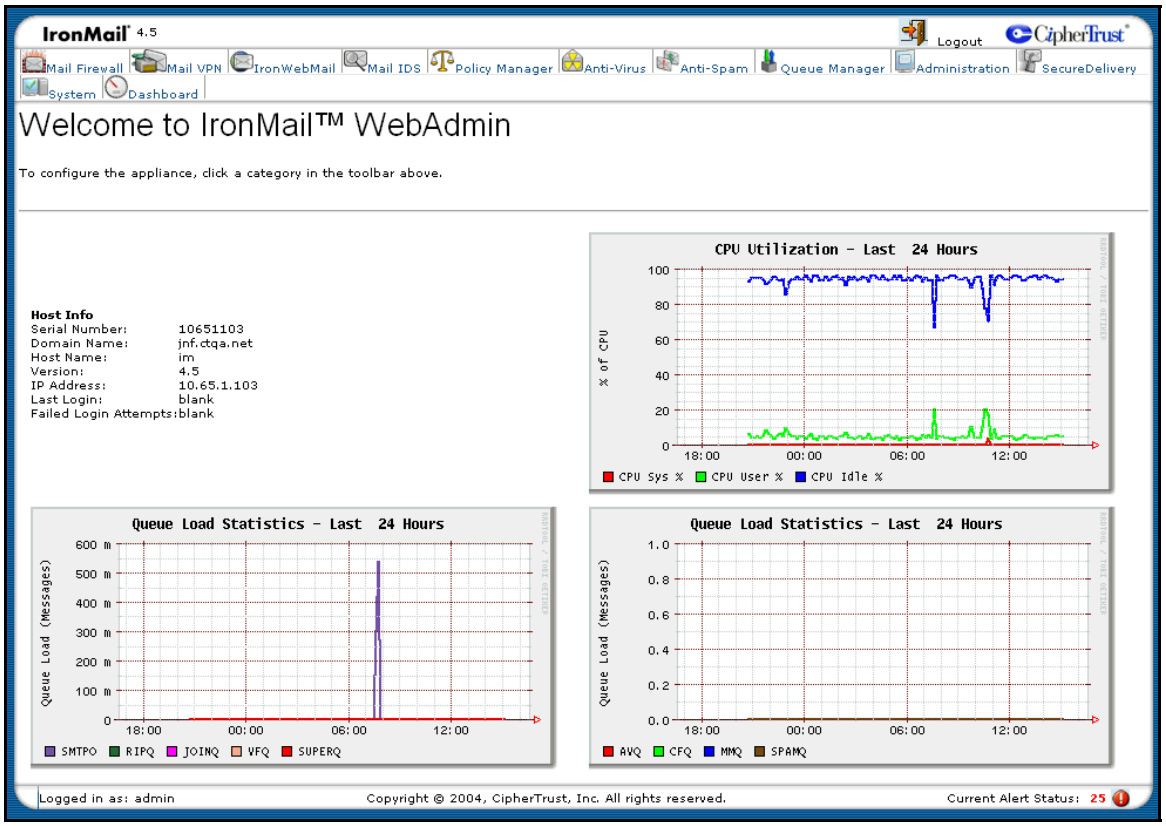
IronMail will automatically restart. The following message will display.


Microsoft Internet Explorer
The appliance is being restarted. This should take 2 minutes. Please wait. In some cases, your browser may return an error. If this happens, please close the browser and return to IronMail login screen.
OK

When the restart process has had time to finish (wait at least three minutes), you may log onto the appliance. Using your network browser, go to the IP address for the appliance and log in.



IronMail's opening screen will display, allowing you to continue with configuration.



Once a stand-alone IronMail is running, it is now acting as a proxy—incoming and outgoing mail will flow through IronMail to the email server you specified, and your exposure to the outside world has been "hardened." However, many of IronMail's features have not yet been enabled. Additional configuration is required as described in the remainder of the *User Manual*.

Configuring IronMail as a CMC

If you configured a *Centralized Management Console*, you must do a few simple tasks before *CMC* can begin minimally managing multiple IronMails:

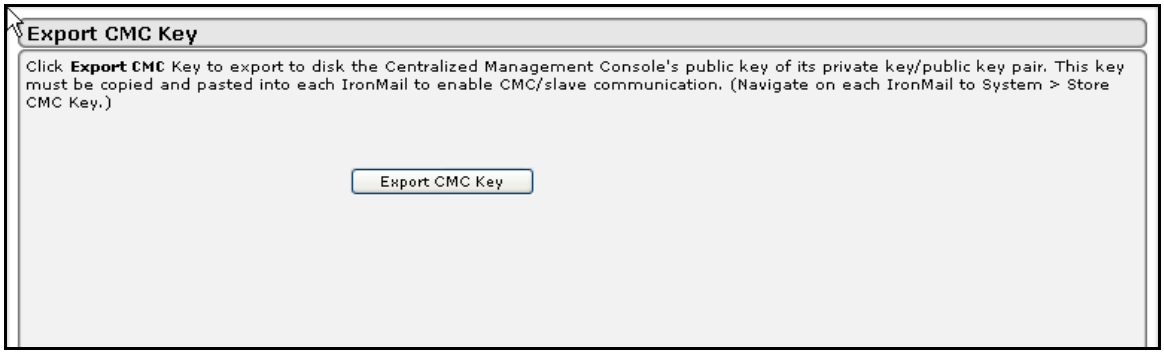
1. You must export the CMC public key of its private key/public key pair.
2. You must install the CMC public key on each IronMail that is to be centrally managed.
3. You must provide the CMC with the host names and IP addresses of each IronMail.
4. You must configure TCP port 20022 on both the CMC and the managed IronMails for CLI access to allow connection between the CMC and the managed appliances and to permit name-based DNS lookups.

Step 1: Exporting the CMC Public Key

Log onto the CMC by entering its *IP address* in your browser. Remember to prefix the IP address with https:// (add the "s" after the "http"). Also, append ":10443" to end of the IP address (specifying the port number through which your browser communicates with the CMC).The address format is: https://<url>:10443.

Enter the default user name and password: "admin" and "password."

Navigate to Centralized Management > IronMail Management > Export CMC Key. Click the Export CMC Key button.


Export CMC Key
Click Export CMC Key to export to disk the Centralized Management Console's public key of its private key/public key pair. This key must be copied and pasted into each IronMail to enable CMC/slave communication. (Navigate on each IronMail to System > Store CMC Key.)
Export CMC Key

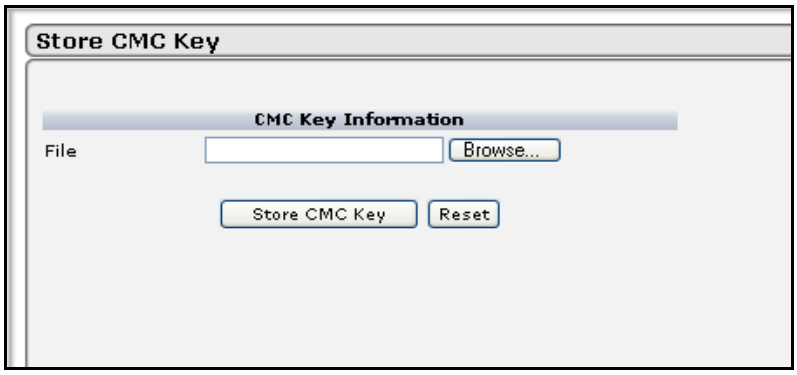
The CMC will create a hyperlink on the page allowing you to download the key (a small text file) to disk. Save the key to a floppy disk or *network* drive accessible by the IronMails to be centrally managed.

Step 2: Installing the CMC Public Key on IronMails

Log onto each IronMail to be centrally managed by entering its IP address in your browser. Remember to prefix the IP address with https:// (add the "s" after the "http"). Also, append ":10443" to the end of the IP address (specifying the port number through which your browser communicates with the CMC).

Enter a valid user name and password (or if running IronMail for the first time, enter the default user name and password: "admin" and "password").

Navigate to System > Store CMC Key.

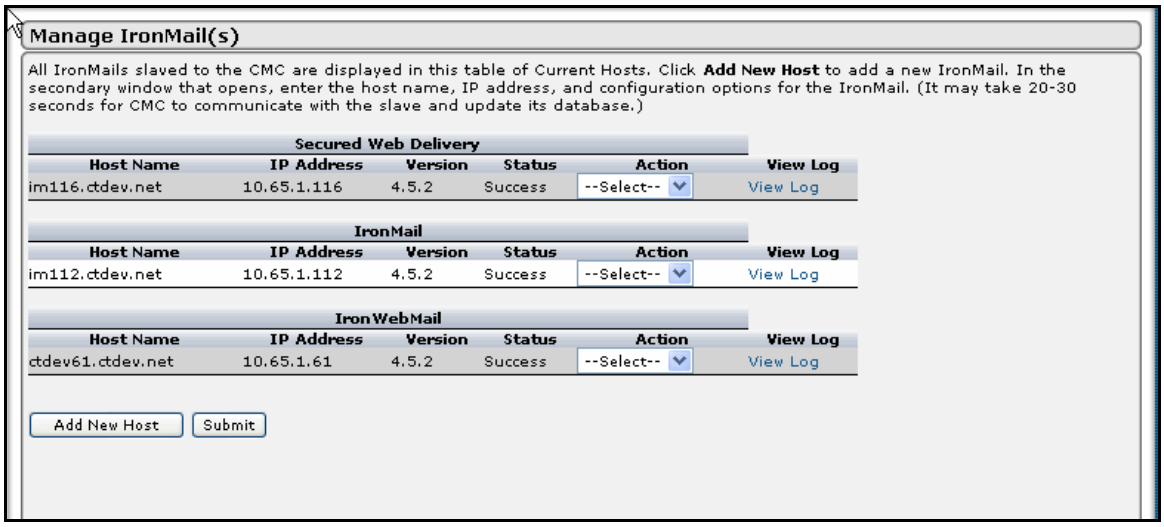


A Browse button on that page of the IronMail interface allows you to navigate to the CMC public key you saved to disk. After selecting the file, click the Store CMC Key button. Ensure that the text "The restore job was submitted." displays at the top of the window, verifying that the CMC key was installed.

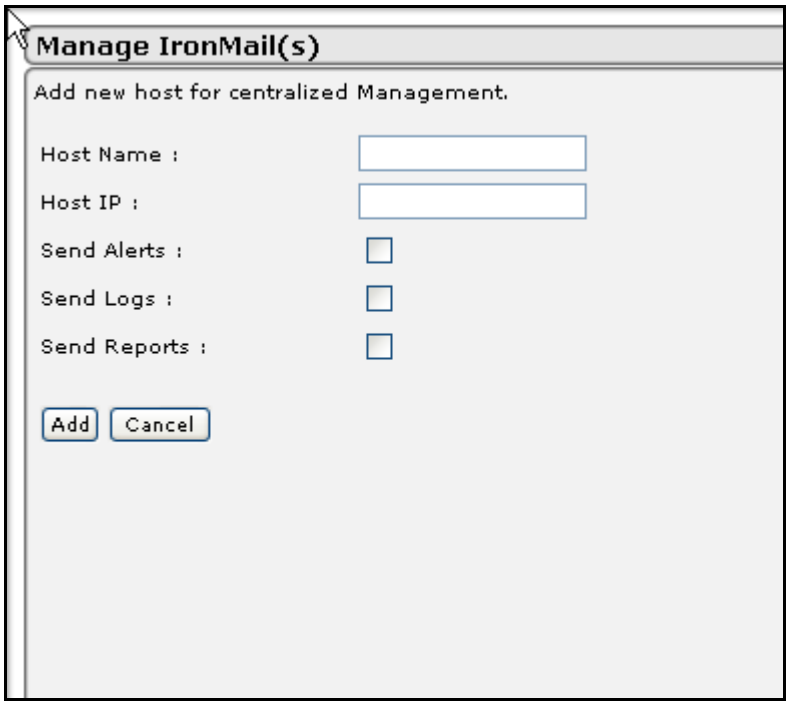
Repeat for all IronMails that are to be centrally managed.

Step 3: Adding IronMails to the CMC

Logon to the CMC and navigate to Centralized Management > IronMail Management > Manage IronMail(s).


Manage IronMail(s)
All IronMails slaved to the CMC are displayed in this table of Current Hosts. Click Add New Host to add a new IronMail. In the secondary window that opens, enter the host name, IP address, and configuration options for the IronMail. (It may take 20-30 seconds for CMC to communicate with the slave and update its database.)
Secured Web Delivery
Host Name IP Address Version Status Action View Log
im116.ctdev.net 10.65.1.116 4.5.2 Success --Select-- View Log
IronMail
Host Name IP Address Version Status Action View Log
im112.ctdev.net 10.65.1.112 4.5.2 Success --Select-- View Log
IronWebMail
Host Name IP Address Version Status Action View Log
ctdev61.ctdev.net 10.65.1.61 4.5.2 Success --Select-- View Log
Add New Host
Submit

Click the Add New IronMail button and enter the *host name* and IP address of an IronMail in the input fields in the secondary browser window that opens. (Select the "Send Alerts" and "Send Logs" options if you want the CMC to receive the IronMail's alerts and log files.)



(After clicking the Add button in this window, an alert message informs you that the CMC's browser interface must restart after the IronMail is successfully added. After closing this alert message, the IronMail is listed in the table of managed IronMails with the word "Adding..." beside it (indicating that CMC is downloading and adding the IronMail information to its own database). If the CMC experiences any difficulty connecting to or downloading data from the IronMail, the word "Failed..." appears beside the IronMail name. After CMC finishes downloading the IronMail data (in ~2-3 minutes), clicking any hyperlink within the user interface will force you to log back into Web Administration.

After logging back into the CMC, return to Centralized Management > IronMail Management > Manage IronMail(s) and click the "View Log" icon displaying in the right column next to the IronMail you just added.

Repeat for all IronMails that are to be centrally managed.

The CMC is now minimally managing the IronMails at this point. That is, the status and activity of each IronMail can be viewed in CMC's Dashboard, and if configured, their log files and alerts will be sent to the CMC. Note that the CMC is intended to allow administrators to create custom *policy* and configuration settings for multiple IronMails, and to "push" product License Keys and file updates to the "slaves." Refer to Centralized Management Console's User Manual for complete instructions on configuring the CMC appliance to centrally manage multiple IronMails.

IronMail has a standard configuration of Maximum Transferred Unit (the maximum size for a single *packet* that may be transferred by the email system) of 1,500 bytes. If your system requires a maximum other than the standard MTU configuration, CipherTrust's Technical Support engineers can accomplish a custom configuration at your request.

Network Connectivity

DNS Configuration

Domain Name Service (DNS) is an exceedingly complex subject, and there is no standard way in which it is implemented. In simple terms, DNS allows multiple servers to appear as if the have the same *host name*. In addition to the DNS server's MX, A, PTR and other records, some networks use *Network* Address Tables (*NAT*) to map servers internally. However you implement DNS, you must at least do the following:

- You must create MX, A and PTR records for the IronMail appliance, and
- You must give IronMail a lower preference number than your mail server's MX record.

This will allow all mail addressed to your domain to be routed to the IronMail appliance, and allow all other servers to perform DNS lookups and reverse lookups on IronMail. The Administrator or Installer names the *DNS Server* during the initial configuration of IronMail. The preference or priority is set after the initial setup, as a System function for configuring IronMail.

The most common use of DNS is to perform "forward lookup" (resolving a fully qualified domain name, such as "servername.yourdomain.com," with a valid *IP address* such as 63.168.166.231). DNS is also capable of "reverse lookup" (resolving an IP address to a fully qualified domain name). The reverse lookup may also be used to detect (and reject) certain kinds of "address spoofing" used by hackers. Most Internet email servers use both of these features.

For a reverse lookup to work, you must publish a reverse zone (e.g., 166.168.63.in-addr.arpa) that contains PTR records mapping IP addresses onto node names. You must create a reverse zone, with your IP address in reverse octet order, followed by the text string "in-addr.arpa." For example, the forward zone is "yourdomain.com" and the reverse zone is "166.168.63.in-addr.arpa."

You can check whether reverse lookup is working using the "nslookup" command. Using nslookup on an IP address with that switch (in-addr.arpa) will do a reverse lookup (IP-to-Host Name), and display the resolved name, as shown below:

```
su-2.04# nslookup 10.0.3.101
Server:  pridocon.ctqa.net
Address:  10.0.3.55
Name:    im.ex.ctqa.net
Address:  10.0.3.101
```

An example of a forward lookup (Host-Name-to-IP) follows:

```
su-2.04# nslookup im.ex.ctqa.net
Server:  pridocon.ctqa.net
Address:  10.0.3.55
Name:    im.ex.ctqa.net
Address:  10.0.3.101
```

Internal Mail Server Configuration

Configuration of your internal mail servers is very simple. Make IronMail the only *IP address* allowed to connect to your mail server, and re-direct your servers' outbound mail flow to IronMail using a static route.

Network Firewall Configuration

Your network administrator must assign an *IP address*, *subnet* mask, and *host name* for the IronMail appliance. (A host name "yourname" and *domain name* "yourdomain.com" results in the

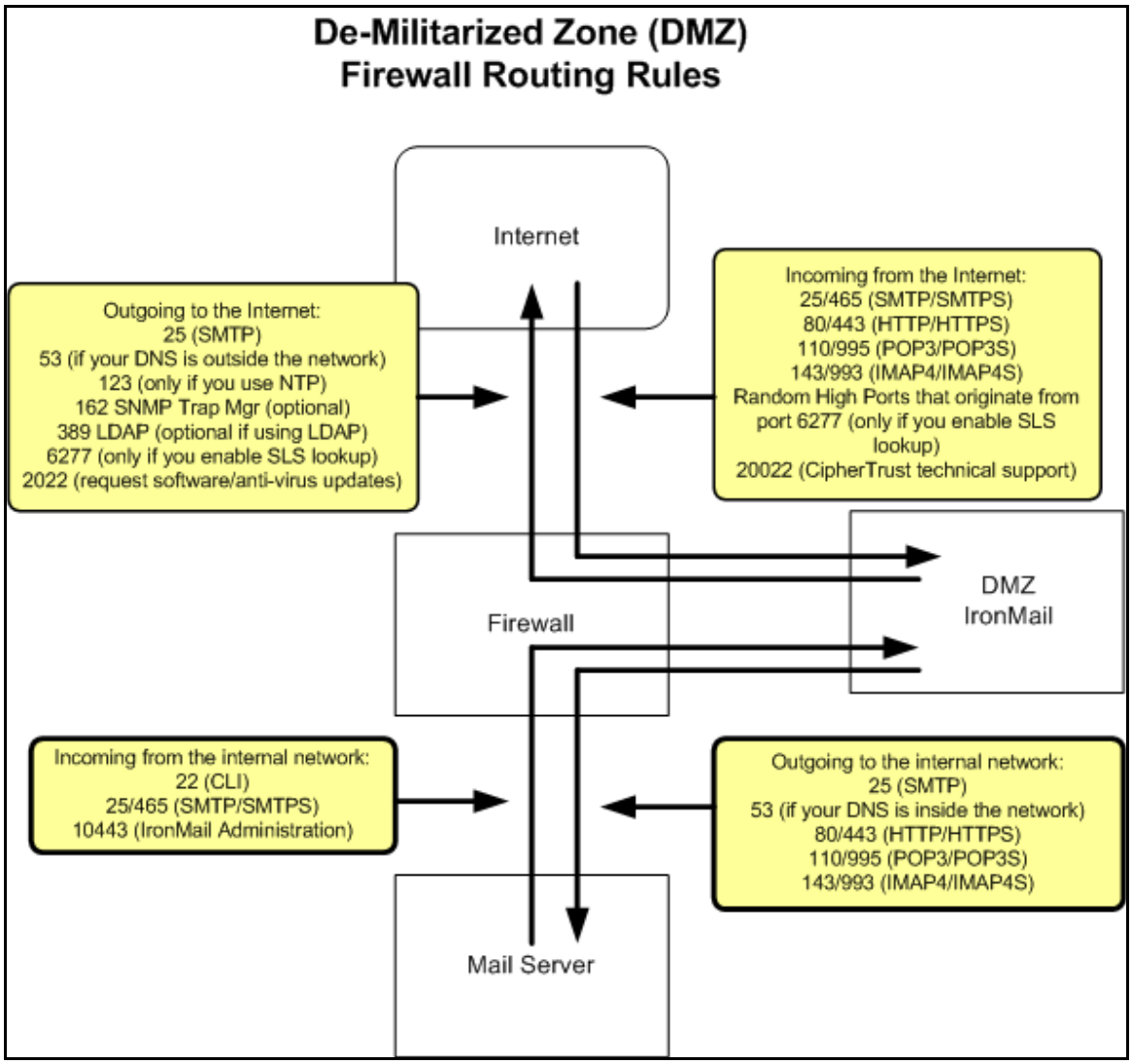
fully qualified domain name (FQDN) “yourname.yourdomain.com.”) The first time you connect to IronMail, you will be required to enter this and other information into its installation wizard. Establishing network connectivity may require the assistance of your network administrator.

Based on your company’s network design, IronMail may be connected to the corporate network either in a De-Militarized Zone (*DMZ*) or on the internal LAN. Once the physical connection has been established, some configuration of the network *firewall* and Domain Name Service (DNS) will be required.

Configuring the Firewall

There are three main styles of firewalls: *packet* filter-types (routers with ACLs), application proxy-types (e.g., Raptor and TIS Gauntlet), and stateful inspection-types (e.g., CheckPoint and Cisco PIX). It is important to understand most application proxy firewalls do not support SMTP over *SSL* (i.e. the SMTPS *protocol*). If your firewall is an application proxy-type that does not support SSL, IronMail will not be able to encrypt your mail. Both packet filter and stateful inspection firewalls, however, fully support SMTP over SSL if they are configured correctly.

It is recommended that you place IronMail in a DMZ if your network supports it. If you do so, you must create rules to allow the protocols for “outside world to IronMail,” “IronMail to outside world,” “IronMail to the internal mail server,” and “internal mail server to IronMail.” There should be no open protocols from outside to inside (bypassing IronMail) when using a DMZ configuration. The following diagram and table describe the ports you must open in your firewall to allow IronMail to function correctly:



A key advantage to the DMZ configuration is that IronMail's analysis of incoming messages is performed before the messages actually penetrate the firewall. IronMail sends its output back to the firewall before it is allowed inside the system. With a non-DMZ placement, incoming messages are inside the firewall before IronMail scans them.

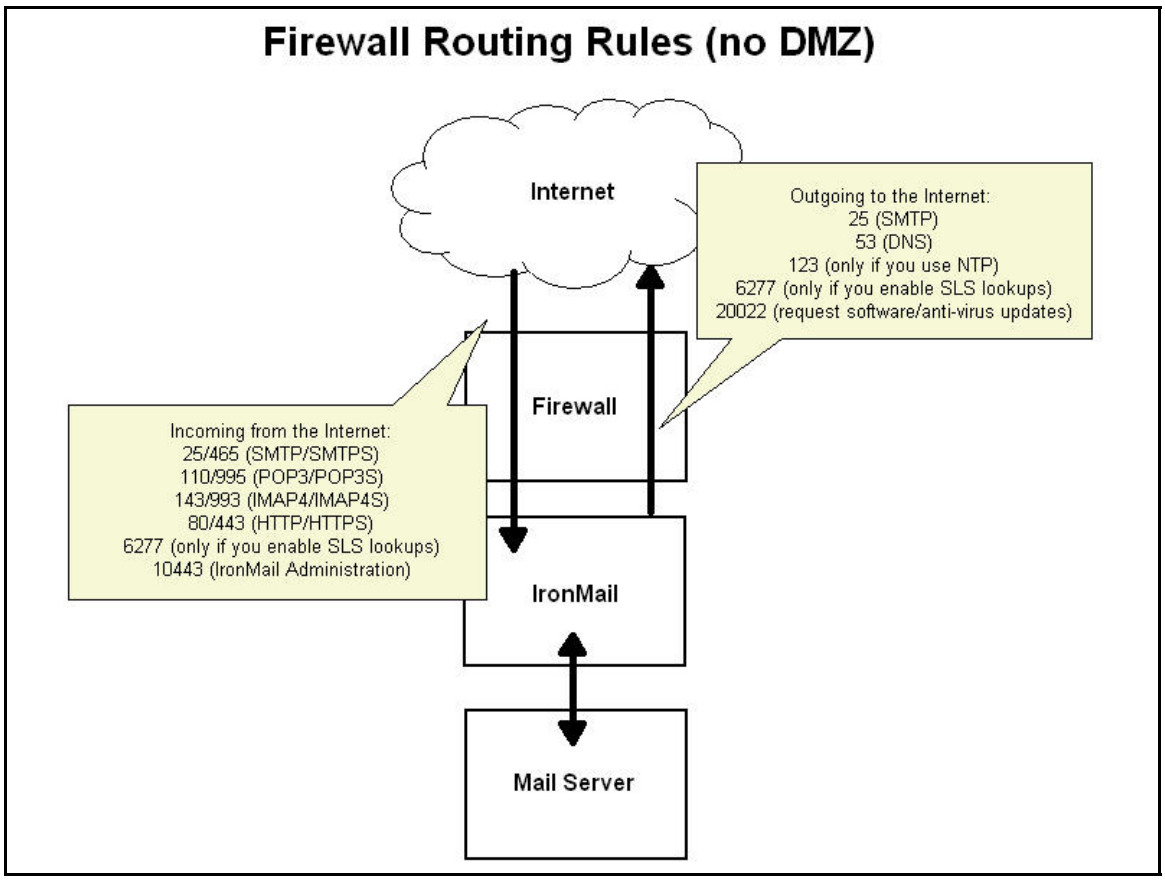
Outgoing-to-the-Internet rules (to allow IronMail to open a connection with the outside Internet):

Port	TCP/UDP	Protocol	Description
Port 25	TCP	SMTP	Required for mail delivery
Port 123	TCP/UDP	NTP	Required if using Network Time Protocol
Port 53	TCP/UDP	DNS	Optional for an IronMail/CMC (if your DNS is outside the network, you must open the port allowing IronMail/CMC to connect to it).
Port 6277	UDP	SLS	Random high port with destination UDP 6277.

Port 20022	TCP	CipherTrust	Required in order for IronMail to request software/anti-virus updates
Incoming-from-the-Internet rules (to allow IronMail to accept a connection from the outside Internet):			
Port 25	TCP	SMTP	Required for mail reception
Port 80	TCP	HTTP	Optional for Web Delivery (secure HTTPS on port 443 is preferred)
Port 110	TCP	POP3	Optional (secure POP3S on port 995 is preferred)
Port 143	TCP	IMAP4	Optional (secure IMAPS on port 993 is preferred)
Port 443	TCP	HTTPS	Optional for Web Delivery (for secure HTTPS proxying)
Port 465	TCP	SMTPS	Optional for secure incoming messages
Port 993	TCP	IMAP4S	Optional (this is the preferred port to securely retrieve mail via IMAP4)
Port 995	TCP	POP3S	Optional (you should open port 995 for secure POP3S instead)
Random High Ports that *originate* from Port 6277	UDP	SLS	Required for IronMail's Statistical Lookup Service spam-blocking tool.
Port 20022	TCP	CipherTrust	Optional (allows CipherTrust to connect to your IronMail for Technical Support)
Outgoing-to-the-internal network rules (to allow IronMail to open a connection with your mail servers):			
Port 25	TCP	SMTP	Required for mail delivery
Port 53	TCP/UDP	DNS	Optional for an IronMail/CMC (if your DNS is outside the network, you must open the port allowing IronMail/CMC to connect to it).
Port 80	TCP	HTTP	Optional for Web Delivery (you should open secure port 443 for HTTPS instead)
Port 110	TCP	POP3	Optional (you should open port 995 for secure POP3S instead)
Port 143	TCP	IMAP4	Optional (you should open secure port 993 for IMAP4S instead)
Port 443	TCP	HTTPS	Optional for Web Delivery (for secure HTTPS proxying)
Port 993	TCP	IMAP4S	Optional (this is the preferred port to securely retrieve mail via IMAP4S)
Port 995	TCP	POP3S	Optional (this is the preferred port to securely retrieve mail via POP3S)

Incoming-from-the-internal network rules (to allow IronMail to accept a connection from your internal network):			
Port 22	TCP	Command Line Interface	Optional (only if you want to access the command line interface from inside the network)
Port 25	TCP	SMTP	Required for mail delivery
Port 10443	TCP	HTTPS	Required (this is the port used to connect to IronMail's WebAdmin interface)

If you do not have a DMZ, it is safe to install the IronMail appliance on your internal network because its hardened face and built-in firewall features protect it. If you install IronMail inside the network, simply open the necessary "port holes" in the firewall. Ensure that your firewall's port settings match the previous table.



Most mail servers use only ports 25, 110, and 143 for sending and retrieving email. However, email transmitted through these ports is unsecured—attackers can read or intercept email sent this way. We recommend that you open the secure ports instead: 995 for POP3S and 993 for IMAP4S to force external users to retrieve their mail via SSL. (IronMail provides the ability to send mail securely on port 25.)

IronMail has a standard configuration for Maximum Transmission Unit (the maximum size for a single packet that may be transferred by the email system) of 1,500 bytes. If your system requires a maximum other than the standard MTU configuration, a custom configuration can be accomplished by CipherTrust's Customer Service group.

GUARDING THE GATEWAY

Gateway Security

The *network* perimeter is, for most corporations, relatively secure. Firewalls, combined with a handful of other tools such as intrusion detection systems (IDS), have established a solid line of defense for corporate networks. In fact, firewalls have been so successful that most attackers have ceased trying to attack them. Instead, hackers are shifting their attacks to areas unprotected by traditional network security tools—to applications such as mail server and web server software. Hackers have learned to use actual email and email protocols as the "carriers" of, or vehicles for, their attacks. Email systems are being widely exploited in order to disrupt and violate corporate networks.

CipherTrust has taken a comprehensive approach to protecting corporations from email risks by providing an integrated solution, deployed at the gateway, which secures every aspect of the email system. It created IronMail, the secure email gateway appliance.

Controlling the Gateway

The first step to achieving email security is control of the gateway. Control the gateway and you protect the entire email infrastructure sitting behind it. But the range of threats targeted at email systems makes control of the gateway difficult. A comprehensive gateway security system must be capable of scrutinizing every attempted Internet connection to your internal servers, as well as the email messages themselves, ensuring that nothing harmful gets through. Such security must be able to stop a hacker's malicious code, a self-propagating worm, or even a dirty joke. If the gateway is secure, attacks never reach the mail servers. IronMail provides this security by fortifying the gateway and scrutinizing everything that attempts to pass through it.

Gateway Threats

Three primary threats plague enterprises if they are allowed to enter through the network gateway:

- Denial of service attacks;
- Intrusions; and
- Web mail attacks.

IronMail provides state-of-the-art solutions for each.

Denial of Service

Hackers may launch denial-of-service attacks against e-mail systems in an attempt to bring those systems to a halt. Many techniques are capable of accomplishing this disruption, but hackers typically exploit vulnerabilities in a mail server, such as the inability to process a malformed *MIME* message or buffer overflow constraints. Or the attackers can simply flood a mail server with more SMTP connections or instructions than the server can handle.

Intrusions

Intrusions occur when unauthorized users gain access to the organization's infrastructure. For spammers, this typically means breaking into a mail server to send spam (mail relay) or to harvest e-mail addresses. Spammers can also plant computer code on the organization's personal computers, which then become spam machines or drones. Recent worms and viruses are examples of the results from intrusions.

Web Mail Attacks

Many enterprises allow their mobile workers to access corporate e-mail through applications such as Outlook Web Access (OWA) or iNotes. Web mail requires a web server, which is subject to numerous vulnerabilities, blended threats, viruses and worms.

IronMail is a hardened e-mail gateway appliance that acts as an application-specific *firewall*. It allows only valid and safe connections to e-mail servers.

CONNECTION SERVICES

Examining Connections

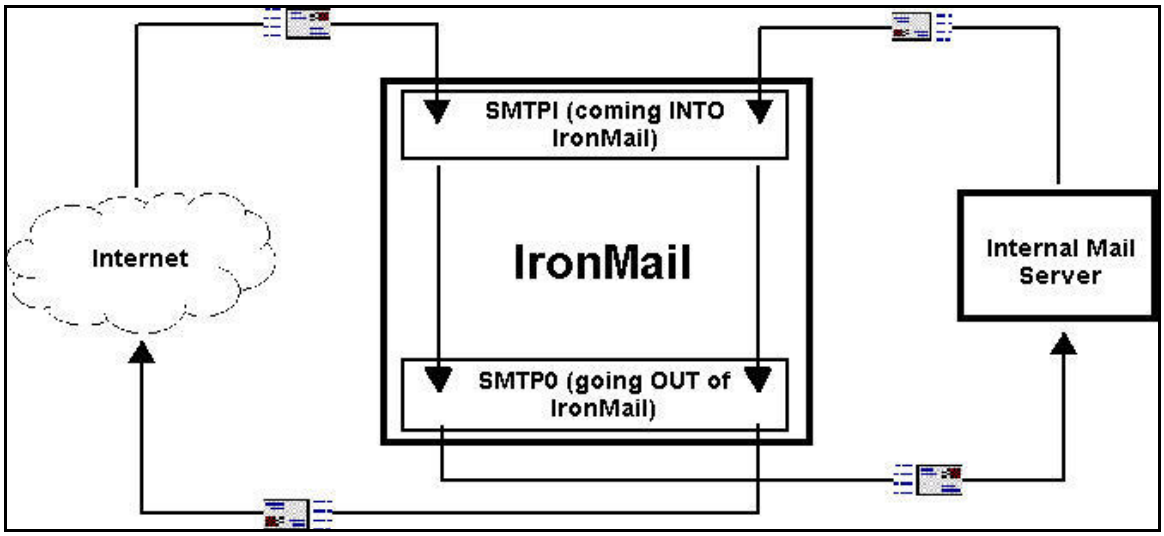
As a proxy, IronMail scrutinizes every attempted connection to your mail servers, detecting and blocking all known or potentially harmful connections. IronMail employs CipherTrust's patented Mail-Firewall® technology to deliver the most robust email gateway protection available.

IronMail's Mail-IDS®, the industry's first email-specific intrusion detection system (IDS), acts like a video camera to proactively monitor the mail servers 24 hours a day. IronMail detects suspicious, mischievous or unauthorized activities. Upon detection, it can notify security managers of impending threats or terminate specific connections to thwart attacks.

The Firewall

Mail-Firewall

IronMail implements three services or "subsystems" to process messages transmitted via the SMTP email *protocol*.

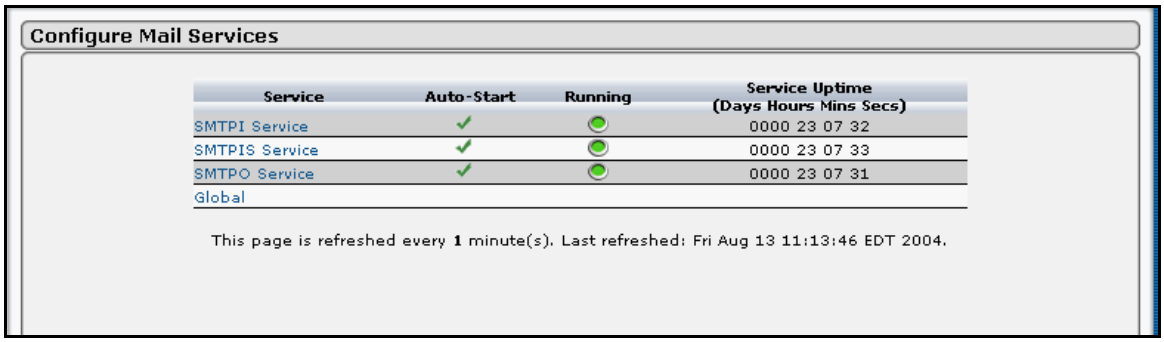


- The **SMTPI Service** processes messages coming into the IronMail appliance via port 25. (The "**I**" signifies "coming **I**nto IronMail.") New IronMail users frequently confuse "incoming messages" with messages coming into the network from the Internet. In fact, the SMTPI Service processes all messages coming into the IronMail appliance, whether originating inside or outside the local network (see SMTPI/SMTPIS Services).
- The **SMTPIS Service** processes messages coming into the IronMail appliance via the secure port 465 (the "**S**" represents "coming into IronMail **S**ecurely"). While email may be transferred securely using the *SSL*/TLS protocol over port 25 using the regular SMTPI service, the SMTPIS service listens for email exclusively on port 465 (see SMTPI/SMTPIS Services).
- The **SMTPO Service** processes all messages that IronMail delivers out of the appliance. (The "**O**" represents "delivered **O**ut of IronMail.") Again, new IronMail users mistakenly think of the SMTPO Service as the subsystem that delivers email originating within the network to users out in the Internet. While this is true, it is more correct to understand that the SMTPO Service delivers all messages out of the appliance, whether their destination is inside or outside the network (see SMTPO Service).

Invisible to the IronMail administrator is the SMTPI and SMTPIS Services' enforcement of the SMTP protocol. Before these services will accept the data or "payload" of an email, they inspect the requested email connection at the application level to ensure that it is legitimate. Connection requests that do not conform to the SMTP protocol are dropped. If the connection is accepted, then IronMail processes the message like a full-featured mail server application. Accordingly, the SMTPI/S Services have many configuration options that affect how they process and deliver messages.

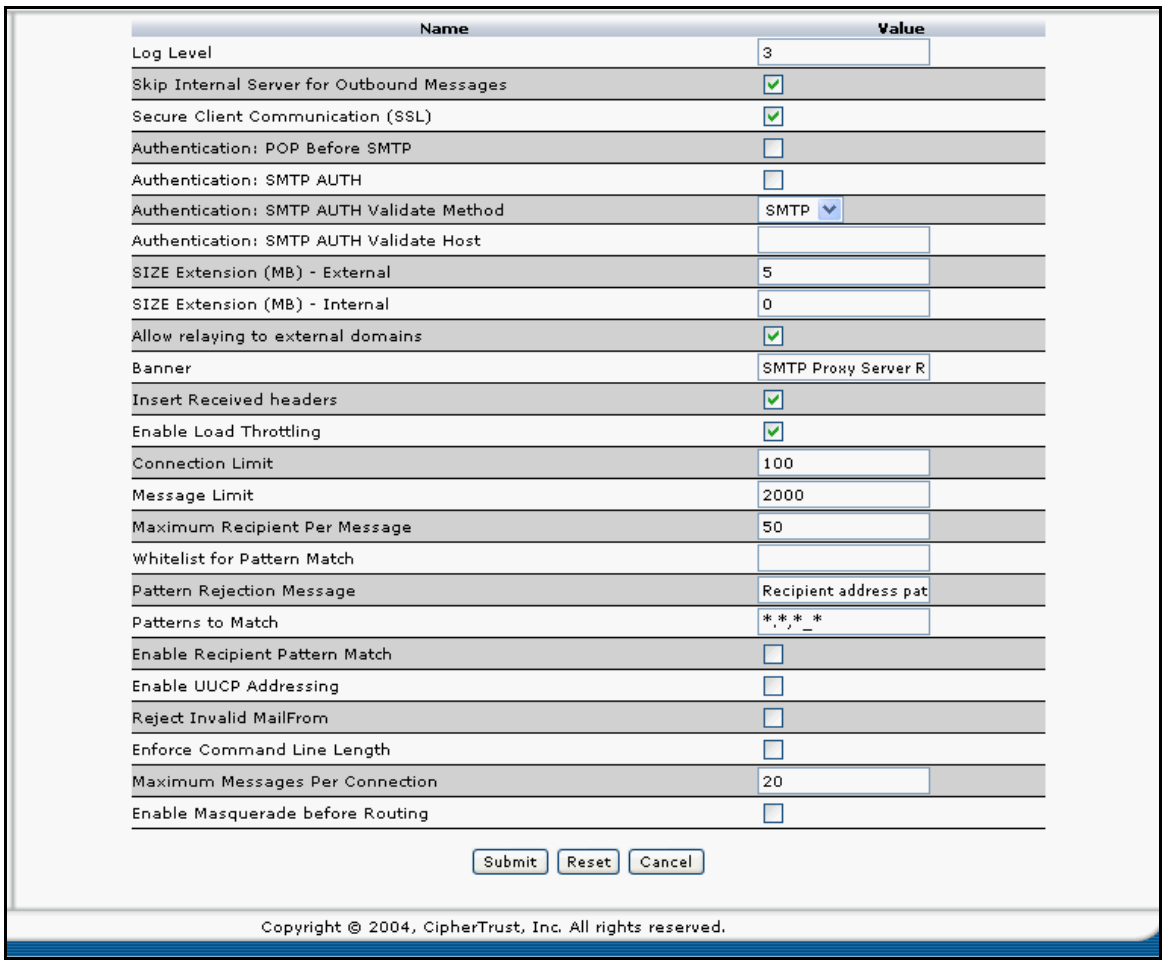
Configuring Mail Services

The Configure Mail Services table contains four columns: **Service**, **Auto-Start**, **Running**, and **Service Uptime**.



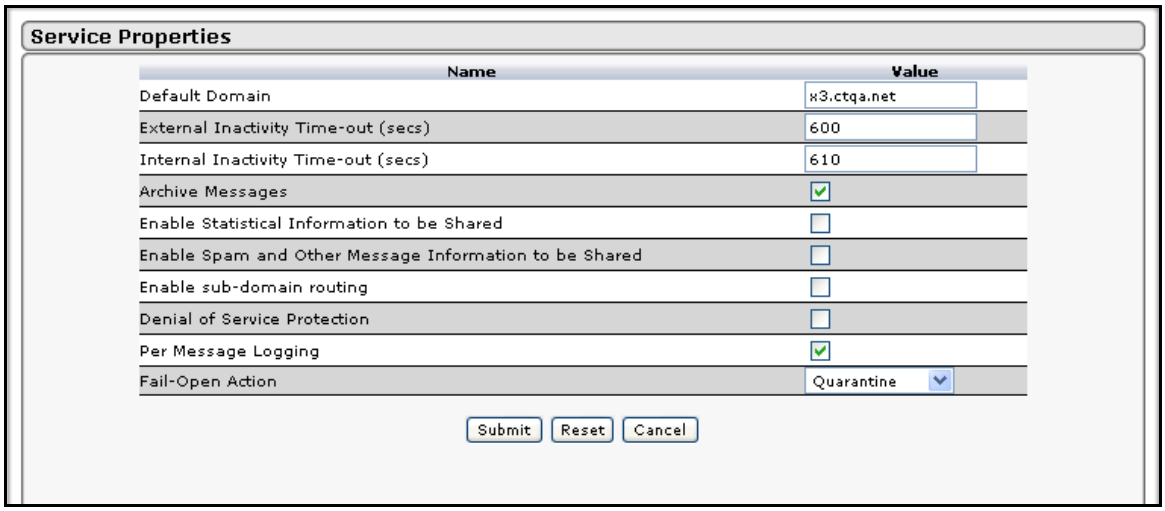
Service	This column contains the names of the IronMail services or subsystems that process SMTP email delivery. (An entry in this column named "Global" allows configuration options that do not strictly fall under the SMTPI, SMTPIS, or SMTPO Services.) Each service name is a hyperlink that allows configuration of that service.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If an icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green, IronMail's Health Monitor will restart any service except SMTPO that has stopped for any reason when it performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off.) The red and green light icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from green to red. If the icon does not toggle as expected, click the Configure Mail Services hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped and restarted by an administrator, or was stopped by an administrator and was restarted automatically by IronMail's Health Monitor.

If you click the hyperlink under Service (the service name), a secondary screen opens showing detailed information about that service. The Administrator may edit the properties on this screen and submit the changes to revise the services.



Global Options

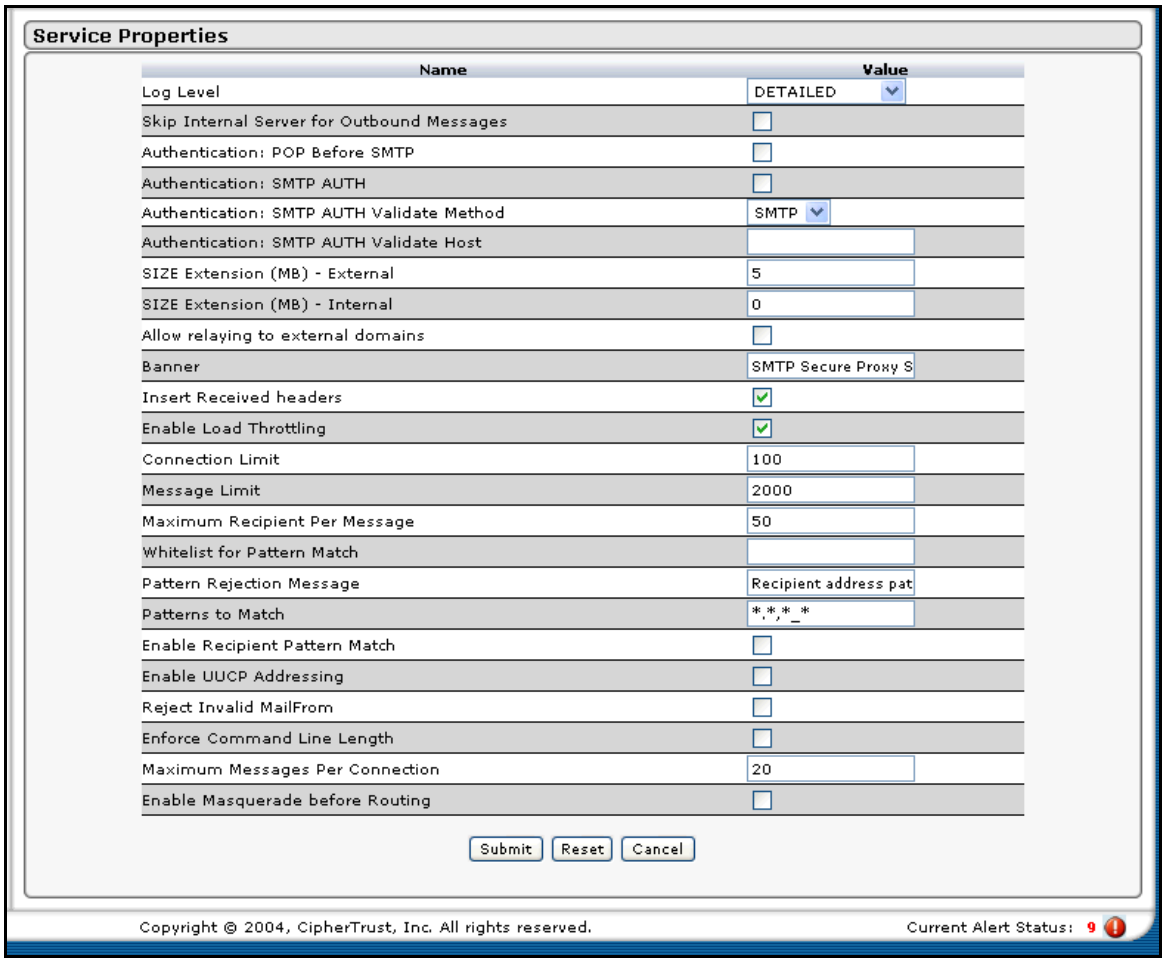
Clicking the Global hyperlink on the last row of the Configure Mail Services table opens a secondary browser window allowing configuration of additional message-delivery options.



Default Domain	By default, the *domain name* provided as the "Default Email Domain" during Step 9 of the Installation Wizard is displayed in this input field. You can edit the field by entering the domain name of the server to which IronMail's administrative messages are to be delivered.
External Inactivity Time-out (secs)	Enter a value representing the maximum number of seconds IronMail may wait for external servers (whether inside or outside the *network*) to respond before closing a connection. It is strongly recommended that the default value of 600 seconds not be changed.
Internal Inactivity Time-out (secs)	Enter a value representing the maximum number of seconds IronMail may wait for its own internal services and subsystems to respond before closing a connection. It is strongly recommended that the default value of 610 not be changed. In any case, this value should be at least 10 seconds greater than the External Inactivity Timeout above.
Archive Messages	If enabled, IronMail will save all incoming and outgoing messages to disk. At approximately midnight each day, when IronMail generates its Reports and Log Files, it will create a zipped tar archive of the messages and, if configured (*Monitoring > Reports/Log Files > Archive*), transport them to an archive server. Note that messages deleted due to an IronMail process (such as enforcement of a Mail Monitoring or Content Filtering *policy*) are not archived.
Enable Statistical Information to be Shared	IronMail will securely transfer statistical information about spam and other trends to be used by CipherTrust Research for research purposes only, and to contribute toward increased effectiveness.
Enable Spam and Other Message Information to be Shared	IronMail will securely transfer spam and other message information to be used by CipherTrust Research for research purposes only, and to contribute toward increased effectiveness.
Enable sub-domain routing	If enabled, IronMail will try to resolve sub-domains to a top-level domain identified in the Domain-based routing table (*Mail-Firewall > Mail Routing > Domain-based*). That is, if messages are addressed to "subdomain.domain.com" and "domain.com" is in the routing table, IronMail will deliver it to the internal mail server mapped to that domain. If this option is not enabled, IronMail will only deliver messages to sub-domains if the sub-domains have been specifically added to the routing table.
Denial of Service Protection	If enabled, IronMail will monitor all TCP connections to all the email ports on which it listens and block future connections for any *IP address* that exceeds the Denial of service threshold. **Note:** We understand that DoS Protection will be removed from this screen, since it also exists within the Mail-IDS configuration.
Fail-Open Action	Select an action from the drop down list for the action to be taken on fail-open (when a message fails to open in ST mode). The options are: • Drop message - deletes the message from processing • Quarantine - places the failed message in the Failures Queue • Pass Through - sends the message on through IronMail's processing

SMTPI/SMTPIS Services

Because the only difference between IronMail's SMTPI and SMTPIS Services is that the SMTPIS Service listens exclusively on port 465 for SSL-secured email while SMTPI Service listens to server-to-server connections on port 25, the properties window for both are nearly identical. The following configuration options are available:



Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the type and amount of detail written to the log. Select the proper log level from the drop down list. The options are: • Critical • Error • Information • Detailed Note that in high email-volume environments (50,000+ messages per day), the SMTPI Service's log can easily grow to 100 MB or more per day. If IronMail is not configured to delete these logs after 3-7 days, there is a danger that IronMail's hard disk can quickly become full.

Skip Internal Server for Outbound Messages	Ordinarily, IronMail will route all messages originating outside the domain(s) it hosts to the internal mail servers. But in instances where external hosts are allowed to relay email through the internal mail servers, enabling this option will relay the messages immediately, without sending them first to the internal mail server. Doing so improves message processing-efficiency by eliminating a "processing step." Bear in mind that unless Mail Relay was enabled in the Allow Relaying to external domains option below (not recommended), IronMail only allows "mail relay" for messages originating from users who can be authenticated by an Authentication Method specified below, or from IP addresses or ranges of addresses in a *subnet* listed in the Allow Relay List (*Mail-Firewall > Allow Relay*). Also be aware that if this option is enabled, messages originating from and destined for an outside domain will bypass any internal hosts that may be in place to perform special processing tasks on messages. And if enabled, internal servers' email statistics may not correspond to actual message traffic.
Authentication: POP Before SMTP	This option allows relaying if a POP request to the internal mail server is accepted. That is, if a user outside the domain attempts to retrieve his or her email from the internal mail server through IronMail, and the mail server accepts the username and password that is submitted during the request, IronMail will also allow that user to send email to external domains. IronMail's *POP3* and/or POP3S Service(s) must be enabled and running in order for the POP Before SMTP authentication to allow relaying. Note that IronMail will "remember" this authentication for the length of time specified in the Denial of Service Window (*Mail-IDS > Application Level > Configure > "Denial of Service Window"*). If a user attempts to send email after the length of time has elapsed, relaying will fail until he or she once again sends a POP request to the internal mail server. Select either this "POP Before SMTP" option or the "SMTP AUTH" option immediately below as a mail relaying validation process. If both are enabled, "SMTP AUTH" takes precedence over "POP Before SMTP."
Authentication: SMTP AUTH	This option allows relaying if an internal authentication server validates the user with an encrypted SMTP method. That is, if this option is enabled and a user attempts to relay mail through the domain, IronMail will connect to the authentication server, proxy the SMTP authentication request, and relay the message only if the user is authenticated. Note that the SMTP authentication server must be running, and have A records in the DNS server so IronMail can find it. And if this option is enabled, the "SMTP Validate Method" and "SMTP Validate Host" must be provided in the input fields immediately below.
Authentication: SMTP AUTH Validate Method	If "Authentication: SMTP AUTH" is enabled above, specify from the **SMTP AUTH Validate Method** pick list whether the authentication server uses a POP or SMTP method.
Authentication: SMTP AUTH Validate Host	If "Authentication: SMTP AUTH" is enabled above, specify the *host name* of the machine running the authentication service. (The host machine must be running, and have A records in its DNS server.)
SIZE Extension (MB) – External	Enter a number (in megabytes) representing the maximum email size IronMail will accept from users outside the domain(s) it hosts. If the message exceeds this size, IronMail will not accept it. A zero in this input field represents "unlimited"—there is no size limit.

SIZE Extension (MB) – Internal	Enter a number (in megabytes) representing the maximum email size IronMail will accept from users inside the domain(s) it hosts. If the message exceeds this size, IronMail will not accept it. A zero in this input field represents "unlimited"—there is no size limit. Bear in mind that though IronMail may accept a large message, the mail server to which the message is addressed may reject it due to its own size restrictions. Also note that users' email clients must convert all binary file attachments to ASCII characters prior to delivery. The conversion will increase the size of the file, roughly, by a factor of 1.4. Therefore, if Windows Explorer reports a file size of 10 MB, the email application will convert it to a ~14 MB file.
Allow relaying to external domains	When this option is enabled, *anyone* may relay email through the domain(s) IronMail hosts. It is not recommended that this option be enabled. It is preferable to selectively allow mail relaying by adding users' or mail servers' IP addresses or subnets to the Allow Relay list (*Mail-Firewall > Allow Relay*), or by enabling "POP Before SMTP" or "SMTP AUTH" authentication (above).
Banner	During an SMTP connection "handshake," email server applications send an SMTP 220 "Welcome Banner," that by default in some cases provides identifying information about the mail server. In order to hide exploitable information about the mail infrastructure, an alternate welcome banner may be used. Enter in the input field a text string to be used as the welcome banner. The banner is limited to 80 bytes of data, and may not contain new line characters (<CR/LF>).
Insert Received Headers	With this option enabled, IronMail will add to every email's header an RFC822-compliant reference to its own role in the delivery of the message.
Enable Load Throttling	IronMail has a very powerful and efficient "engine" capable of processing tens of thousands of messages very quickly. However, in very high email environments, or during times of peak volume, IronMail can dynamically "throttle" the rate of incoming connections based on how many messages have already been received and are still in the process of being examined. As the number of unprocessed and "still-being-processed" messages grows, the SMTP Service will begin lowering the numbers of simultaneous email connection requests it accepts. When IronMail reaches an administrator-defined "maximum message load" (see immediately below), the SMTP Service drops to its default low-acceptance rate of three simultaneous connections (see the Load Throttling graphic below). As the message load decreases, the rate of simultaneous incoming SMTP connections increases again. When IronMail's load throttling is in effect, users trying to send mail to domains IronMail hosts will receive a "421: Server busy. Try again..." alert message in their email client if their connection is refused. The load throttling parameters are established by the **Connection Limit** and **Message Limit** fields that follow.
Connection Limit	Enter a number (1-200) representing the maximum number of simultaneous incoming SMTP connections IronMail allows. IronMail will dynamically throttle backward from this number. (Administrators may wish to monitor their daily volume of email for one or more weeks before setting this value. Review the corporate *firewall* Connection Log for port 25 to see what typical simultaneous connection rates are.)

Message Limit	Enter a number (500-50,000) representing IronMail's "maximum message load." (A zero is not allowed in this field.) When this number of "not yet processed" and "in-process but not yet delivered" messages is present in IronMail's Message Store, the SMTP Service will drop to its lowest connection acceptance rate of three simultaneous connections. Load throttling gracefully slows the number of accepted simultaneous connections, from the number established as the "Connection Limit" down to a default low of three simultaneous connections, depending on how closely the number of messages in the Message Store approaches the Message Limit specified here.
Maximum Recipients Per Message	Enter a number (25-500) representing the maximum number of recipients to which an email may be addressed. (The SMTPI and SMTPIS Services total the sum of all recipients, regardless of whether they are contained in the TO, COPY, or BLIND COPY fields.) For IronMail-to-IronMail communications, if an email is addressed to 200 addresses and the SMTPI recipient limit is set to 50, IronMail will accept the message and deliver it to the first 50 recipients submitted by the sending server. The SMTPI Service will not deliver the message to the 51st recipient and beyond. If the email is received from a non-IronMail server, the behavior can differ and IronMail may reject the entire message where the number of addresses exceeds the SMTPI limit.
Whitelist for Pattern Match	Enter a list of valid email addresses (case insensitive) for which the pattern match check should not occur. Pattern matching is bypassed if the recipient address is present in the list. Separate each address in the list by a comma using no space separation. This field can contain up to 16,000 characters including the separators (commas).
Pattern Rejection Message	Enter the text that is to be part of the SMTP Failure (550) response (indicating that the Mailbox is unavailable) when an inbound recipient address does not match the specified patterns.
Patterns to Match	Enter the pattern or patterns that a recipient's email address is allowed to have. Either or both of the two patterns (*.* and *_*) are permitted. Patterns must be separated by a comma (,) with no space separation between the comma and the pattern.
Enable Recipient Pattern Match	This option enables pattern checking. Only two patterns are currently supported. The configured pattern(s) are used to inspect the unique message identifier (UID) part of the recipient email address: • *_* eg. *firstname_lastname*. The UID has at least one underscore "_" as in the recipient email address, james_smith@earthlink.com. • *.* eg. *firstname.lastname*. The UID has at least one period "." as in the recipient email address, account.manager@ciphertrust.com. By default this option is disabled. If this option is enabled, a pattern match check is performed using the patterns in the **Patterns to Match** field. If a pattern match occurs, IronMail returns an OK (250) reply response. Otherwise IronMail returns a Failure (550) reply.
Enable UUCP Addressing	If enabled, IronMail allows UUCP (Unix-to-Unix CoPy) addressing. UUCP is a computer program and *protocol* allowing remote execution of commands and transfer of files, email, and netnews between Unix computers. If disabled, IronMail rejects the recipient.
Reject Invalid MailFrom	If enabled, as part of spoofed message protection, IronMail will reject mail from an address that is part of a routing domain, but is not in the Allow Relay IP addresses.

Enforce Command Line Length	IronMail will enforce RFC restrictions on the length of an SMTP command line to 512 characters, including carriage returns and line feeds.
Maximum Messages per Connection	Enter a number (0 - 50) to represent the maximum number of messages allowed per connection. Entering zero (0) enables an unlimited number of messages. The limit applies only to connections that do NOT have relay permission through IronMail.
Enable Masquerade before Routing	If enabled, IronMail will perform Address Masquerade functions before routing validations.

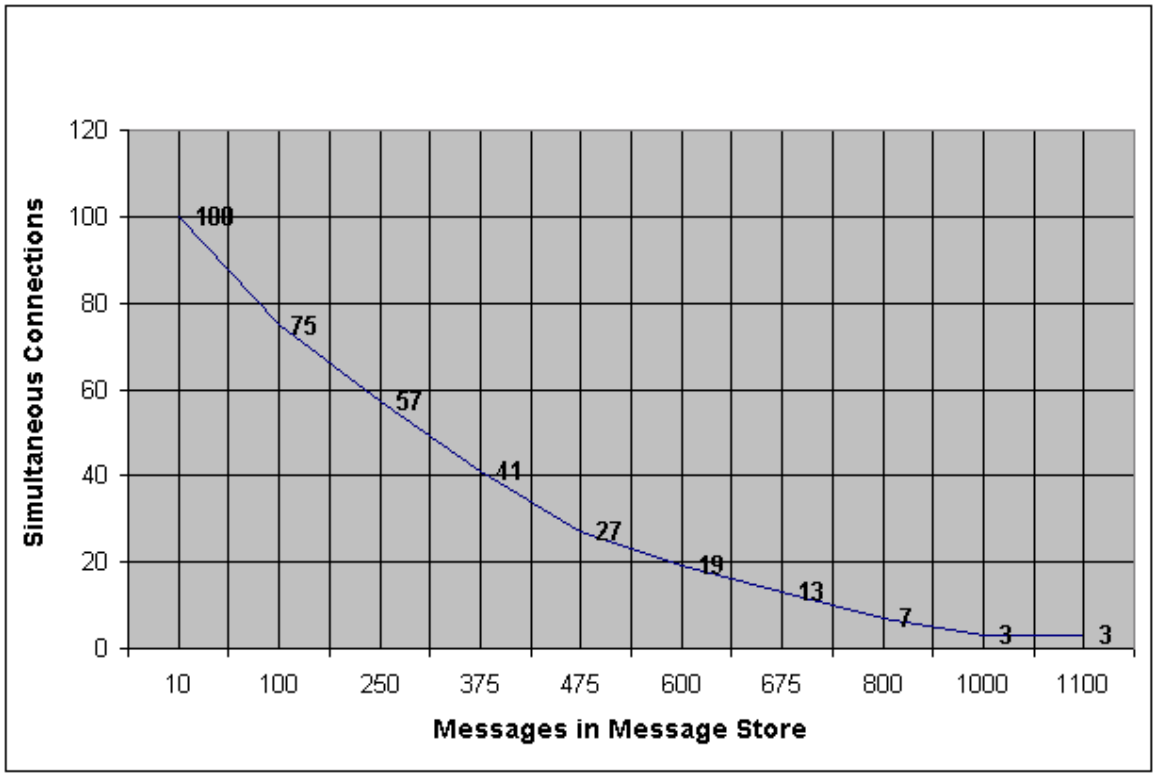


Illustration of Load Throttling

Note: When the **Submit** button is clicked after any configuration change, SMTPI and SMTPIS processes are reconfigured and the configuration changes take effect for connections established after the change.

Spoofed Message Protection

IronMail provides administrators the ability to reject any email with the user's own domains in the "Mail From" field, unless that message comes from a server that exists on the Allow Relay list. This functionality can be applied at either the SMTP level or as part of the System-Defined Header Analysis rules.

Detection takes place in the Mail From Command of the SMTP *protocol*; action may be taken in SMTPProxy or in the Spam Queue. IronMail can be configured to drop the message immediately (in SMTPProxy) or accept the message and mark it as a forged domain for SDHA to act.

Important! This function may stop legitimate email for internal users when they use an external source to generate mail and send it using IronMail. This feature should be used caution and forethought.

The SMTPI Service versus the SMTPIS Service over Port 465

In Server to Server and Client to Server communications over port 25 (processed by the **SMTPI Service**), the connection begins in plain text, and the connecting host determines if the two servers should negotiate an *SSL* connection. When the two servers negotiate an SSL connection, they do not open a new port or change the connection they are using. The existing connection is used, and the connection is converted to an SSL connection. Here is the process:

Sending Server > Connects > Receiving Server (Port 25)

Receiving Server > Sends BANNER > Sending Server

Sending Server > Sends EHLO <*DOMAIN NAME*> > Receiving Server

Receiving Server > Sends Capabilities (including SSL or STARTTLS) > Sending Server

Sending Server > Sends TLS or START TLS command > Receiving Server

Receiving Server > Acknowledges the command.

Receiving Server and Sending Server negotiate Session Key for SSL connection and socket is now encrypted

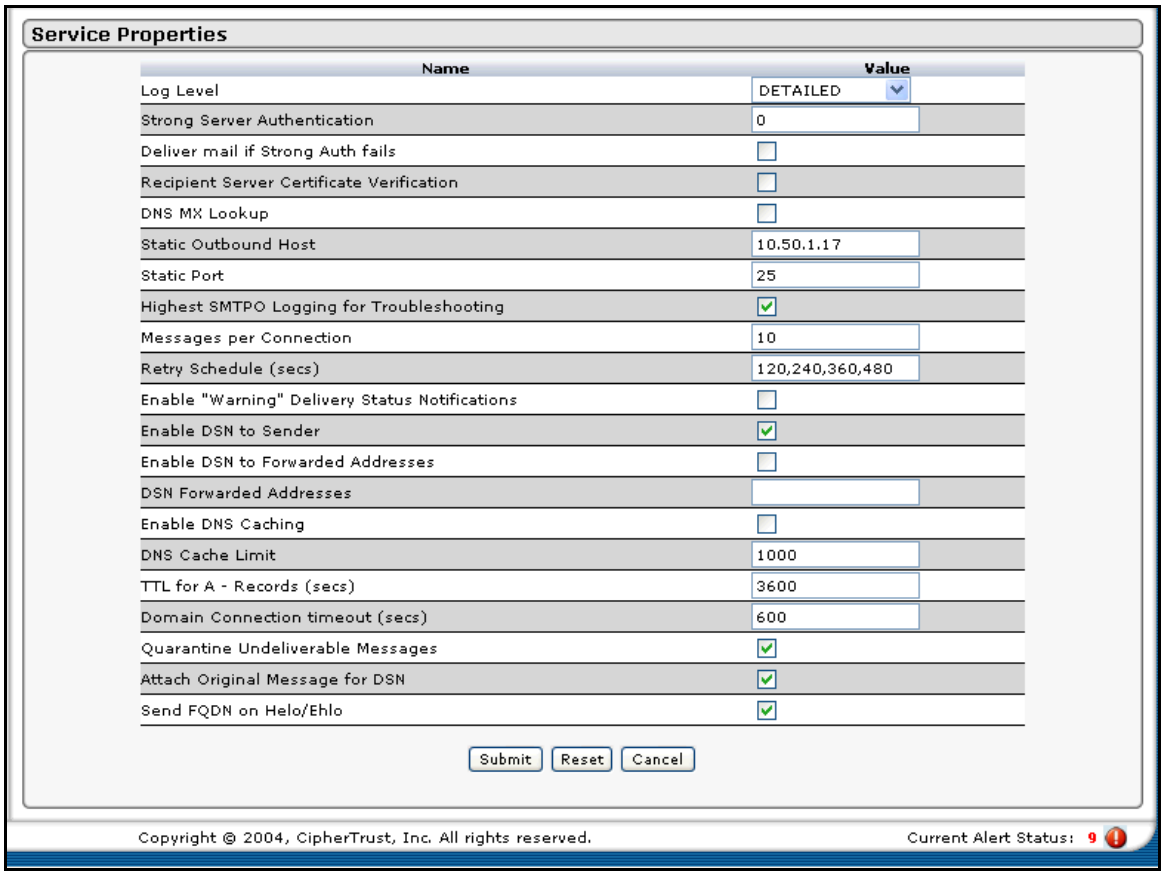
Sending Server > Sends EHLO <DOMAIN NAME> > Receiving Server

Mail flow happens same as normal connection, except all email is encrypted in the SSL socket

IronMail's **SMTPIS Service**, however, is used specifically for Client email programs—when a client email application is configured to connect to the IronMail appliance on port 465 to send email securely. On this type of connection, there is no TLS or STARTTLS. The TLS connection is negotiated at connection time when the SMTPIS Service receives a connection request on port 465, and all commands and email are sent encrypted. This port is generally NOT used for server-to-server SMTP email.

SMTPO Service

Whereas the SMTPI and SMTPIS Services are responsible for processing messages entering the IronMail appliance (whether originating from inside or outside the hosted domain), the SMTPO Service is responsible for delivering the messages out of the appliance (whether the recipient is inside or outside the hosted domain). Clicking the SMTPO Service hyperlink in the Configure Mail Services window opens a secondary browser where the following configuration options are available:



Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the type and amount of detail written to the log. Select the proper log level from the drop down list. The options are: • Critical • Error • Information • Detailed Note that in high email-volume environments (50,000+ messages per day), the SMTPI Service's log can easily grow to 100 MB or more per day. If IronMail is not configured to delete these logs after 3-7 days, there is a danger that IronMail's hard disk can quickly become full.

Strong Server Authentication	Receiving servers may have Security Certificates installed on them and support TLS. Yet the presence of a Security Certificate does not guarantee authenticity. Therefore, in accordance with the values entered in this input field, IronMail may refuse to deliver a message to any server that cannot "strongly" authenticate itself with a valid Security Certificate. There are three possible values for this option: • "0" (disabled, i.e. no authentication required) • "1" (require a Security Certificate, perform a TLS HandShake, and verify that the receiving server's *host name* the common name (host name) on the its security certificate.) • "2" (require a Security Certificate, perform a TLS HandShake, and verify that the receiving server's *domain name* matches the domain name on its security certificate.) **Note:** If a "1" or "2" is entered in this input field and the receiving server does not have a valid Security Certificate, the email will not be delivered unless the very next option, immediately below, is enabled. It is important to state very plainly: as long as there are few servers with installed Security Certificates, the chance that this option will cause valid email to be undeliverable will be very high. This option only becomes useful as increasing numbers of servers install valid Security Certificates. Therefore, IronMail administrators are cautioned to be judicious in their implementation of this option.
Deliver Mail if Strong Auth fails	If a value of "1" or "2" is entered in the "Strong Server Authentication" option above, and the host or domain name on the receiving server's Security Certificate cannot be authenticated, this option determines whether or NOT IronMail will deliver the message. If unchecked, messages will not be delivered when the Security Certificate cannot be authenticated. If checked, IronMail will deliver the message regardless of the certificate's authenticity.
Recipient Server Certificate Verification	If enabled, this option requires the strongest possible server authentication before sending messages: IronMail will validate the Security Certificate with the trusted "root" source that issued it. This verifies that the "root" of the receiving server's Security Certificate is a valid Certificate Signing Authority (CSA). If this option is enabled and verification fails, the connection will be dropped. If the option is disabled, a verification failure will be logged, but the connection is allowed and the message will be delivered. The "verification failure" event is logged in the "SMTPO Service" daily detailed log file.
DNS MX Lookup	If enabled, IronMail will use a DNS MX lookup to identify where to send email it is to deliver. IronMail uses the DNS servers whose IP addresses are listed in *System > Configuration > IronMail > "DNS-1," "DNS-2," and "DNS-3."* If disabled, IronMail will deliver all email to the address in the **Static Host** field identified immediately below. (The **DNS MX Lookup** and **Static Host** options are only valid for messages that are delivered to external domains.) **Note** To prevent potential looping and blocking conditions, IronMail does not attempt delivery of email if the MX lookup returns the reserved *IP address* (0.0.0.0 or 127.0.0.1).

Static Outbound Host	Instead of performing a DNS lookup and delivering messages accordingly, IronMail can send all messages to a specific host that may perform special processing or routing functions. (The host then becomes responsible for the delivery of messages.) Enter either the host name (e.g., "hostname.domainname.com") or IP address of the server where IronMail should deliver all its messages. (If entering a host name, IronMail must be able to resolve the name to the machine's IP address, i.e. DNS records must exist for it.) Note that domains and machine names in IronMail's routing table (*Mail-Firewall > Mail Routing > Domain-based*) take precedence over the route that is specified here in the SMTPO properties window. Any messages addressed to a domain listed in the Domain-based routing table will be delivered directly to that domain's mail server, rather than to the Static Host identified here. To ensure that a host processes all messages IronMail has to deliver, either remove all SMTP entries in the Domain-based routing table, or rename the machine name entries for the SMTP *protocol* in that table to the machine name or IP address of the Static Host identified here. The **DNS MX Lookup** and **Static Host** options are only valid for messages that are delivered to external domains.
Static Port	If IronMail is configured to deliver all its messages to a Static Host (immediately above), provide in this input field the port number on which IronMail must make the connection.
Highest SMTPO Logging for Troubleshooting	IronMail maintains a log, saved to disk, recording the actions of the SMTPO subsystem. By default, the logging level is set to "Medium"—recording useful information, but not detailed information. During times when maximum information describing how the SMTPO Service processes messages is required, enable this option. Note that logging at this level provides highly detailed information about every email that is processed. In high-volume mail environments (50,000+ messages a day), the daily SMTPO log file can easily grow to 100 MB or more, raising the risk that hard disk space may quickly become consumed. This option should only be enabled for the period of time during which troubleshooting is occurring. Once the need for detailed logging has concluded, this option should be disabled.
Messages per Connection	Specify, the maximum number of messages IronMail will deliver to a single domain over one connection. For example, if this value is set to "10" and there are 25 messages addressed to Yahoo.com, IronMail will open three connections with Yahoo and send 10 messages in two of the connections, and 5 messages in the third. Note that many servers interpret high numbers of messages on a single connection as Spam and may be configured to drop the connection. The default value of "10" messages per connection is generally acceptable for most environments.

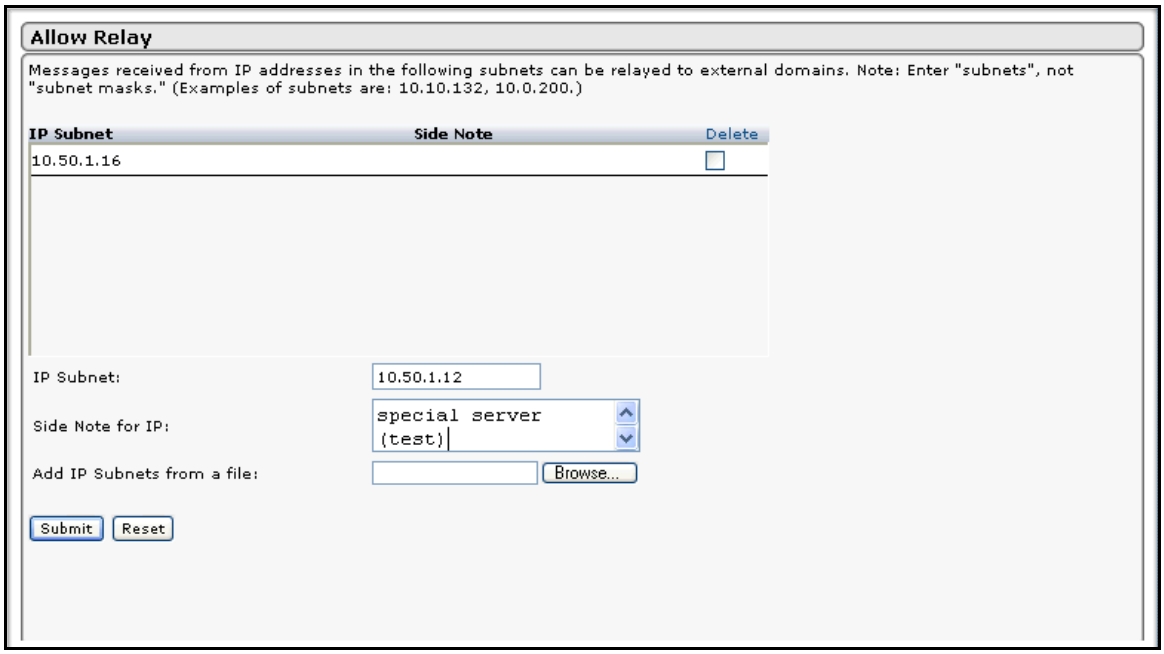
Retry Schedule (secs)	If the receiving server cannot accept a message the first time it is delivered, IronMail can make four additional attempts to deliver it. Enter four numbers, in ascending order, separated by commas. (IronMail requires four values.) Each value represents the number of seconds after the first failed delivery that IronMail should wait before attempting another delivery. IronMail's default values mean it will make its second attempt 15 minutes after the first failure, its third attempt 4 hours after the original failure, its fourth attempt 24 hours after the original failure, and its final attempt 48 hours after the original failure. After the final failed delivery, IronMail will drop the message. Note, however, that if "Quarantine Undeliverable Messages" is enabled below, IronMail will quarantine undeliverable messages. Administrators have the opportunity to "resend" the quarantined undeliverable messages (with five attempted deliveries each) as many times as they want.
Enable "Warning" Delivery Status Notifications	If this option is enabled, IronMail will send a Delivery Status Notification (DSN) message each time it is unsuccessful in delivering a message. If this option is not enabled, IronMail will only send a DSN after its final delivery attempt was unsuccessful. "Enable DSN to Sender" must be enabled immediately below in order for these "warning" DSN messages to be generated.
Enable DSN to Sender	If this option is enabled, IronMail will generate a Delivery Status Notification (DNS) message if it is unable to deliver a message. If enabled and "Enable Warning Delivery Status Notifications" is disabled, the DSN will be generated after the final delivery attempt. If enabled and "Enable 'Warning' Delivery Status Notifications" immediately above was also enabled, DSNs will be generated after each failed delivery attempt.
Enable DSN to Forwarded Addresses	Delivery Status Notifications may be delivered to one or more individuals in addition to the message sender if this option is enabled and valid email addresses are provided in the input field immediately below.
DSN Forwarded Addresses	If "Enable DSN to Forwarded Address" is enabled above, DSNs may be delivered to one or more addresses entered in this input field. Enter valid email addresses separated from each other by commas. (Do not enter spaces between commas and subsequent email address.)
Enable DNS Caching	If enabled, IronMail will cache the MX records provided by a DNS query for domains to which it delivers messages. The MX record remains in cache until the MX record's time-to-live (TTL) has expired, after which IronMail deletes it. Caching MX records may provide improved performance, because it reduces the need to perform an MX lookup for each mail delivery.
DNS Cache Limit	Enter a number (between 100 and 2500) representing the maximum number of MX records IronMail will store in its cache. Every 5 minutes, IronMail will delete MX records whose DNS-specified TTL has expired. When the administrator-defined limit has been reached, IronMail will not allow any additional MX records into its cache until its cleanup process deletes old records.
TTL for A-Records (secs)	While the TTL for MX records is defined by the *DNS server*, the TTL for A records is administrator-defined. Enter a number (in seconds) representing how long the A records should live in IronMail's cache. (3600, or one hour, is a recommended setting.) IronMail will delete A records whose TTL has expired.

Domain Connection timeout (secs)	Enter a number (between 300 and 900) representing the maximum number of seconds IronMail may wait for a domain to accept a connection. If a connection cannot be established within this time, IronMail will fall back to the Retry Schedule (above) for additional delivery attempts. (Timeouts may occur if domains are very busy, or a DNS server is unable to respond with the necessary information.)
Quarantine Undeliverable Messages	If a "retry schedule" was configured above, IronMail will make up to five attempts to deliver a message. If this option is not enabled, IronMail drops the message after the fifth attempt. If this option is enabled, IronMail will quarantine undeliverable messages to an SMTPO "Quarantine Queue." (Access quarantined undeliverable messages at *Queue Manager > Outbound Queue > Quarantined Messages*.) From the SMTPO Quarantine Queue, administrators may re-send the messages, so that IronMail makes up to another five attempts to deliver it.
Attach Original Message for DSN	Select this option if the original message is to be attached for DSNs generated. If this option is not selected, only headers of the message are attached.
Send FQDN on Helo/Ehlo	If this option is enabled, IronMail will send the Fully Qualified Domain Name when it establishes a connection.

Note that if IronMail has been configured to require *SSL* message delivery to specific domains (*Secure Delivery > Boundary-to-Boundary > External > SSL*) and the receiving server cannot support SSL, IronMail will "fall back" to Secure Web Delivery if that feature/license has been installed and the domain has been configured to use it. Otherwise, IronMail will not deliver the message—it will send a Delivery Status Notification indicating that it could not deliver the message.

Allow Relay

IronMail's SMTPI and SMTPIS Services both provide an option to "allow relaying to external domains" (*Mail-Firewall > Configure Mail Services > "SMTPI Services" & "SMTPIS Services"*). Ordinarily, this option should never be enabled as it allows anyone in the world to send email through the domain's mail server. IronMail will only accept mail for delivery outside the network if it originates from an *IP address* or *subnet* that appears in this Allow Relay table. Therefore, this table should contain the IP addresses of all internal mail servers that IronMail hosts, as well as addresses and subnets of users outside the network who may have a legitimate need to relay their mail through the network. The IP addresses of the IronMail appliance and the default mail server (provided during the Initial Configuration Wizard) are listed by default.



Field	Description
Table Headers	The table in the upper portion of the screen displays subnets through which messages may be relayed to external domains. The information shown includes: • IP Subnet - the IP address for an approved mail server • Side Note - lists the information entered using the "side note" options below • Delete - a checkbox allowing deletion of any (or all) IP subnets **Note:** If the "Valid sub-domain" option is enabled in User Spam Reporting, enter the subnets of all internal users. Otherwise, they will not be able to report spam to IronMail.
IP Subnet:	In this field, enter the IP address for an IronMail-hosted mail server to be added.
Side Note for IP:	Enter descriptive text, as desired, to identify the IP subnet being added.
Add IP Subnets from a File:	If a file contains IP Subnets in text format, they may be uploaded into the Allow Relay list. The import file should contain one or more lines in the following format: `IP_subnet|IP_sidenote` *Where* **IP_subnet** is a 32-bit (four-octet) IP address or classful subnet. This value is required. *Where* **IP_sidenote** is any alphanumeric comment. This value is optional. The sidenote may contain simulated carriage returns if " " is inserted at the desired location. Multiple "spaces" may be added to the sidenote by replacing the space with its HTML equivalent: " ".

Note that when an IP address is placed on the Allow Relay list, it will not be evaluated for Denial of Service attacks. This may be a potential vulnerability.

Mail Routing

IronMail provides several capabilities for routing email. Email addressed to a specific domain may be mapped to a specific internal mail server. An LDAP directory's information may also be used to specify how mail is routed—IronMail will look up the LDAP server information and route the message accordingly. Plus, administrators must explicitly specify which of their internal servers may send messages through IronMail to the outside world. (Unless internal mail servers are identified in the Internal Routing list, IronMail will not deliver their mail to external recipients.)

The Mail Routing hyperlink in the left navigation frame expands to offer Domain-based, LDAP-based, and Internal sub-menus.

Domain-based Routing

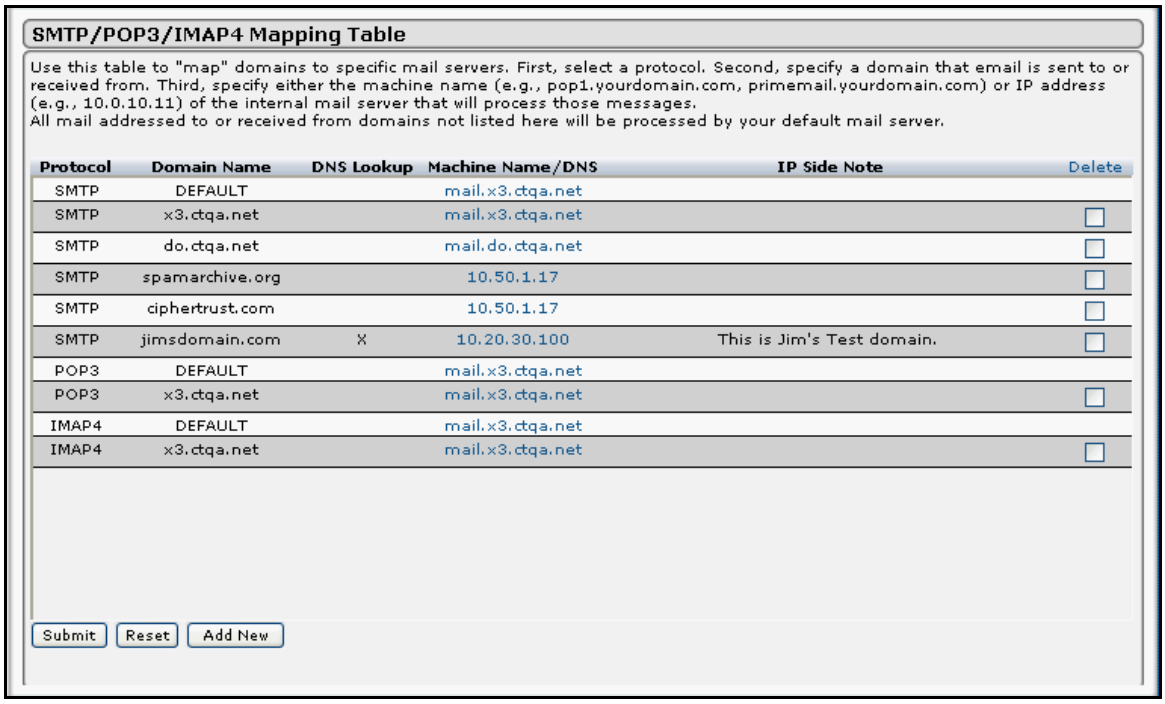
Specific domains or sub-domains may be mapped to specific internal mail servers. All messages to that domain or sub-domain will be delivered to the specified machine name (internal mail server).

CipherTrust recommends you limit each single IronMail appliance to routing mail to a maximum of 100 internal domains.

IronMail uses the following logic to deliver the message:

1. Use LDAP routing information if LDAP routing is enabled.
2. If LDAP is not enabled, or if LDAP does not provide a route, use the sub-domain route existing in this table.
3. If a sub-domain route does not exist in this table, deliver it to the mail server hosting the next-level of the destination domain. (For example, if "name.subdomain.domain.com" does not exist in the Mapping Table, IronMail will look for "subdomain.domain.com." And if that entry is not in the table, IronMail will look for "domain.com.")
4. Step three repeats until the top-level domain (e.g., "domain.com") is reached.
5. If the *IP address* sending the message is not on the Allow Relay list (*Mail-Firewall > Allow Relay*), IronMail (SMTPI) responds with a "571 Cannot relay" message, and the connection is dropped.
6. When Skip Internal Server for Outbound Messages (*Mail Firewall > SMTPI & SMTPIS Services > "Skip Internal Server for Outbound Messages"*) is enabled and a message is addressed to a domain not mapped in this Mapping Table, IronMail verifies that the message sender is identified in the Allow Relay List and relays it. (If not on the Allow Relay List, IronMail drops the message.)
7. When "Skip Internal Server for Outbound Messages" is disabled, all messages will be delivered internally, and if the recipient's domain is not in the Mapping Table, the email is routed to the default domain.

To change the default mail server, enter a list of host names or IP addresses separated by commas in the "Machine Name" column for the Default entries for the SMTP, *POP3*, and *IMAP4* protocols. Additional internal mail servers may be added to this list as the number of internal mail servers which IronMail protects, increases.


SMTP/POP3/IMAP4 Mapping Table
Use this table to "map" domains to specific mail servers. First, select a protocol. Second, specify a domain that email is sent to or received from. Third, specify either the machine name (e.g., pop1.yourdomain.com, primemail.yourdomain.com) or IP address (e.g., 10.0.10.11) of the internal mail server that will process those messages.
All mail addressed to or received from domains not listed here will be processed by your default mail server.
Protocol
Domain Name
DNS Lookup
Machine Name/DNS
IP Side Note
Delete
SMTP DEFAULT mail.x3.ctqa.net
SMTP x3.ctqa.net mail.x3.ctqa.net
SMTP do.ctqa.net mail.do.ctqa.net
SMTP spamarchive.org 10.50.1.17
SMTP ciphertrust.com 10.50.1.17
SMTP jimsdomain.com X 10.20.30.100 This is Jim's Test domain.
POP3 DEFAULT mail.x3.ctqa.net
POP3 x3.ctqa.net mail.x3.ctqa.net
IMAP4 DEFAULT mail.x3.ctqa.net
IMAP4 x3.ctqa.net mail.x3.ctqa.net
Submit
Reset
Add New

Protocol	This column shows the mail service (SMTP, IMAP4, or POP3) for the domain. • SMTP: protocol for sending email. • POP3: protocol for retrieving email. • IMAP4: protocol for retrieving email
Domain Name	Lists the domain or sub-domain name that IronMail hosts in the corresponding user input field.
DNS Lookup	An "X" in this column indicates that DNS lookup is enabled for the domain.
Machine Name/DNS	This column shows the fully qualified machine name or IP address of the mail server responsible for the domain's mail. More than one machine name (or IP address) may exist to provide better routing. "Fail-over" occurs in the order in which the machines are listed in this field.
IP Side Note	This column lists any explanatory or descriptive notes that were configured when someone added a new domain or edited an existing domain.
Delete	To remove mapping of a domain to an internal server, check its **Delete** box and click **Submit**.

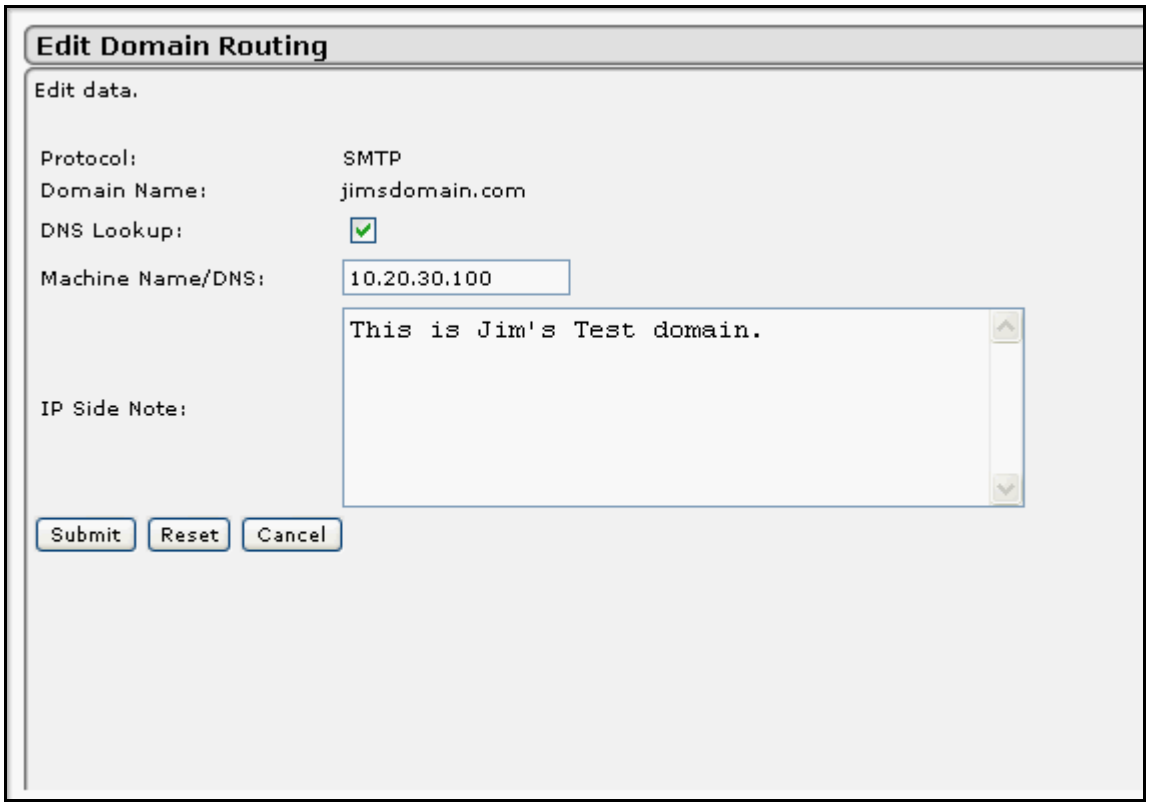
If a message is addressed to a domain not mapped here, IronMail will drop the connection—the message will not be accepted—unless the sender is on IronMail's Allow Relay List, or the message sender has been authenticated by a POP Before SMTP or SMTP AUTH method.

If mail exchange servers are added to this mapping table after taking a "snapshot" of internal mail servers' MX and A records (*Monitoring > DNS Hijacking*), administrators must remember to return to DNS Hijacking and update IronMail's copy of these records by taking a new "snapshot."

Click the machine name/DNS hyperlink to edit an existing domain listing, or click the "Add New" button to insert a new domain routing. Click "Submit" to save all changes when the information is correct.

Edit Domain Routing

Clicking the Machine Name/DNS link on the mapping table opens the Edit screen shown below.



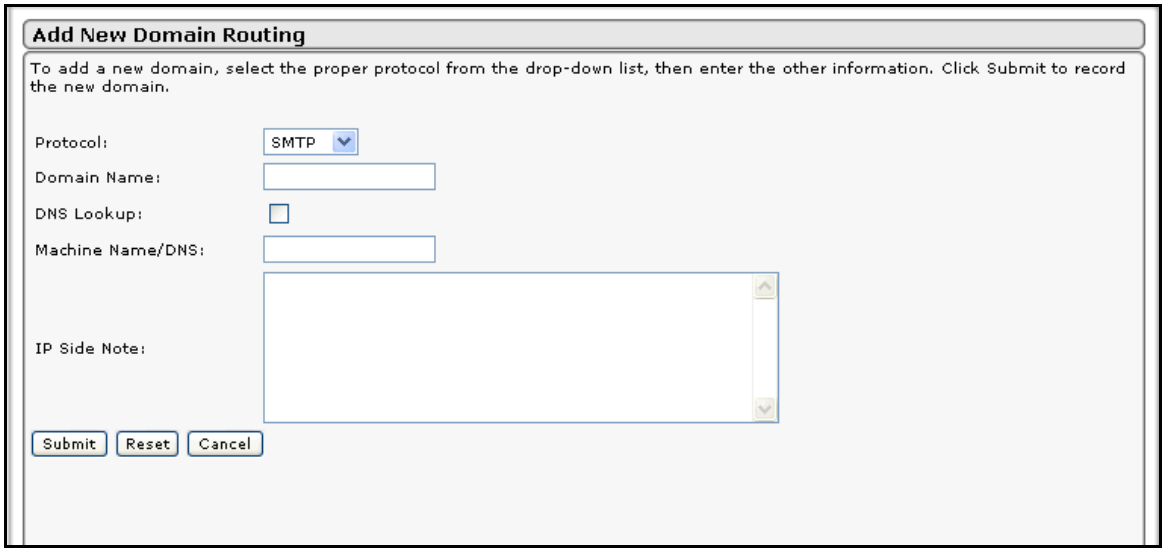
You can edit the following items on the screen:

- DNS Lookup,
- Machine Name/DNS, and/or
- IP Side Note.

When the editing is complete, click "Submit" to save the changes.

Add Domain Routing

Clicking the "Add New" button on the mapping table allows you to add an new domain routing to the list, using the screen below.



Protocol	From the list, select the mail service (SMTP, *IMAP4*, or *POP3*) for the domain. The options are: • SMTP: protocol for sending email. • POP3: protocol for retrieving email. • IMAP4: protocol for retrieving email
Domain Name	Enter the domain or sub-domain name that IronMail will use to host the domain.
DNS Lookup	Checking the click box enables DNS lookup for the domain.
Machine Name/DNS	Enter the fully qualified machine name or *IP address* of the mail server responsible for the domain's mail. More than one machine name (or IP address) may be added to provide better routing. Separate the machine names or IP addresses with commas and *without spaces* between the commas and the subsequent name or IP address. "Fail-over" occurs in the order in which the machines are listed in this field.
IP Side Note	Enter any explanatory or descriptive notes that should appear in the mapping table.

Click "Submit" to save the new domain when the information is complete.

LDAP-based Routing

IronMail can use the information in any LDAP-compliant directory for various functions, including mail routing and *policy* management. Examples of an LDAP-compliant directory include Microsoft Active Directory, Lotus Domino Directory, Groupwise eDirectory and Sun ONE Meta-Directory (formerly iPlanet).

1. **Use LDAP for user-based mail routing:** If each user object contains an attribute with its next-hop SMTP server, this information can be used by IronMail to effectively determine the mail routing path.

2. **Use LDAP for group-based mail routing:** IronMail will use an LDAP server's group information by routing mail to the group's next-hop SMTP server.
3. **Use LDAP for Policy Manager groups:** IronMail can pull user-specified group information back the LDAP server. The groups can then be used anywhere in IronMail where groups may be specified, such as in Policy Management and Anti-Spam.
4. **Validate only (no mail routing) - use LDAP to accept mail only for users who exist in the internal domain:** Messages will only be accepted into IronMail for users that exist in the LDAP directory. No routing information will be used. Routing will be handled by the domain-based routing rules.

In IronMail 4.5, it is possible to use the LDAP server for both mail routing tasks like "Validate Only" and other tasks like synchronizing group information.

Note: Selecting a "Use LDAP-based Routing" command does not actually enable LDAP routing; it enables the LDAP query to the LDAP database.

Using LDAP for *email routing purposes* is set in this LDAP-based Routing window. LDAP configuration for *group management* is set in IronMail's *Policy Manager > Group Manager >* *LDAP* window.

LDAP-based Routing List
Select Use LDAP-based routing when you want to access information on your LDAP server. (Enter your LDAP server, name, and port.) If your LDAP server is not configured for groups, select Use user-based LDAP. (LDAP will be used for routing only.) If your LDAP server is configured for groups, select Use group-based LDAP. (LDAP will be used for both routing and Group Management.) Enter other information as requested.
Use LDAP
Use user-based LDAP routing
Use group-based LDAP routing
Reject Non-LDAP Recipients
Validate Only
LDAP Server:
10.50.1.20
LDAP Port:
389
Authentication
User:
cn=Directory Manage
Password:
Base String:
dc=x3,dc=ctqa,dc=ne
User String:
mail=%%SMTP%%
Email Attribute:
mail
Mailhost Attribute:
mailhost
Submit
Reset

Screen for User-Based LDAP Routing

LDAP-based Routing List
Select Use LDAP-based routing when you want to access information on your LDAP server. (Enter your LDAP server, name, and port.) If your LDAP server is not configured for groups, select Use user-based LDAP. (LDAP will be used for routing only.) If your LDAP server is configured for groups, select Use group-based LDAP. (LDAP will be used for both routing and Group Management.) Enter other information as requested.
Use LDAP
Use user-based LDAP routing
Use group-based LDAP routing
Reject Non-LDAP Recipients
Validate Only
LDAP Server:
10.50.1.20
LDAP Port:
389
Authentication
User:
cn=Directory Manage
Password:
Base String:
User String:
mail=%%SMTP%%
Email Attribute:
mail
Mailhost Attribute:
mailhost
Submit
Reset

Screen for Group-Based LDAP Routing

Note: When configuring group-base information, enter the LDAP details in *Policy Management > LDAP-based Routing List*. The LDAP-based Routing List page contains a number of user input fields:

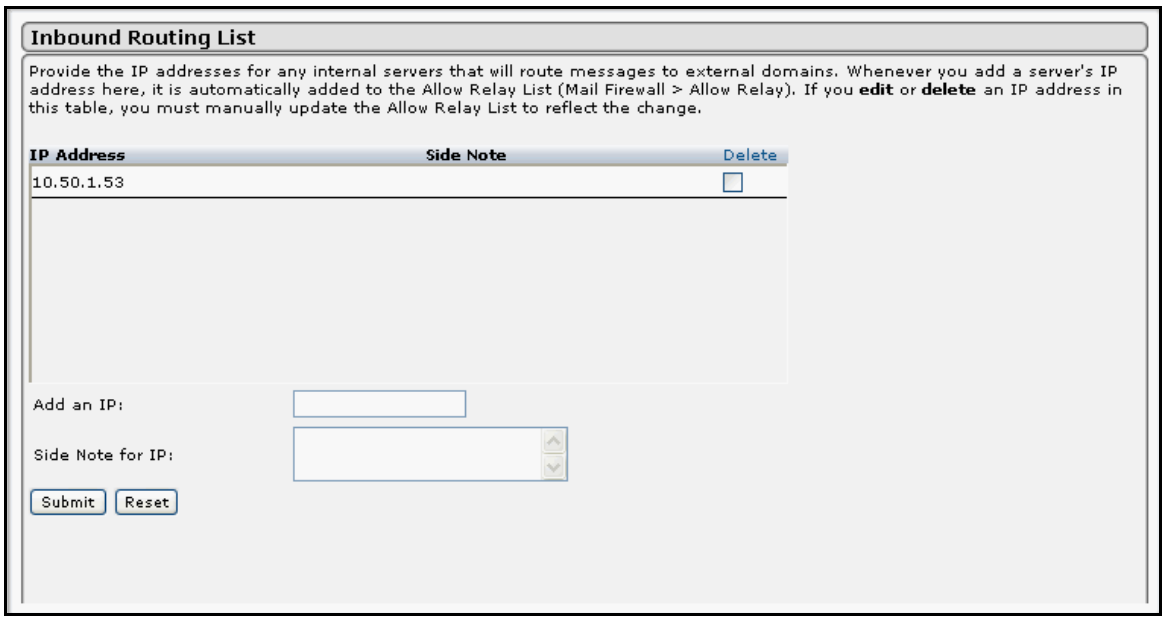
Use user-based LDAP Routing	Enable LDAP routing by checking this option. IronMail will look up the routing information in an LDAP database when delivering mail to end users. This is also the option to use for a Validate Only action (see below). Mechanism: During the SMTP RFC821 session, when IronMail recieves a "RCPT TO" command with an email address, IronMail does a real-time user-based lookup. It sends a query to the LDAP server to see if there is a mathc for the RCPT TO email address. The attribute that is matched is the Email Attribute. The MailHost attribute is requested by IronMail to be used as the next-hop SMTP gateway for that user. The MailHost attribute must return a hostname or an *IP address*. If the LDAP server finds the email address, it returns the MailHost attribute, and IronMail will use that as the place to which to send the message. If the LDAP server cannot find the email address, no MailHost attribute is sent, and IronMail fails over to domain-based routing for that address.

Use group-based LDAP Routing	IronMail will query the LDAP server to see if the user belongs to a group with routing information. The groups are synchronized back to IronMail so that the routing information is taken from those groups and not done via a real-time query to the LDAP server. Mechanism: IronMail queries the LDAP server beginning at the "Base String" and requests all the objects specified by the "Group String" (LDAP filter string). The query requests the attribute specified by "Group Attribute" and the "MailHost" attribute. The group attribute is usually the "member" or "uniqueMember" attribute. This attribute contains the list of Distinguished Names (DNs) that belong to the group members. The MailHost attribute should contain the next-hop SMTP server to be used for all users found in that group. IronMail initiates a second set of queries using each user's DN in turn as the new base string, but this time requesting the email attribute. This attribute is the location where the user's email address is stored, and is often named "mail." IronMail then creates groups using the group's Common Name field populated with the users' email addresses.
Reject Non-LDAP Recipients	If you have chosen to use user-based routing, IronMail provides the ability to reject any RCPT TO address that is not contained in the LDAP server. This option applies only if you are using **user-based LDAP routing**.
Validate Only	Select this option if you wish to validate users against the LDAP directory without having to configure user-based routing. If you choose this option, mail routing will not be used. The LDAP information should be entered in the same way as for user-based routing. Mechanism: IronMail uses the "User String" field to determine if the user exists on the server. If the LDAP server finds the email address, it returns the mailhost attribute, and IronMail allows the RCPT TO for the user and returns a 250 response. It the LDAP server does not return the mailhost attribute and the search is a failure, IronMail returns a 550 error to the RCPT TO command. The sending SMTP server can continue to send RCPT TO commands for that transaction per the 821 *protocol*. Currently, the mailhost attribute field is used to verify a returned LDAP record. The record only needs to exist, and for Validate Only, the information is not used for any other purpose. The mailhost attribute must point to an attribute that exists for all valid users, such as the mail attribute itself.
LDAP Server and Port	Enter the *host name* or the IP address of the LDAP server and the port IronMail must use to connect to it. The well known LDAP port (and the IronMail default) is 389. IronMail does not currently support LDAP over TLS.
Authentication	Enter the user name and password required to authenticate (bind) to the LDAP directory. The user name should be in the DN format. Example: cn=administrator,dc=domain,dc=com. Leave this field empty to initiate an anonymous bind to the server.
Base String	This string defines the starting point in the LDAP schema for the search. Choosing an appropriate base string can save time and processing resources. It is best to specify the exact branch where the users or groups exist rather than specifying the top level of the directory. Example: ou=users,o=CipherTrust is better than simply o=CipherTrust.

User String	This string is used for Validate Only operations. It can be used to query a single attribute or multiple attributes. The string "%%SMTP%%" will be replaced with the RCPT TO address and sent to the server as a filter. Example: If the LDAP server held users' email addresses in both the mail and proxyMail attributes, the user string would be entered as follows: (|(mail=%%/SMTP%%)(proxyMail=%%SMTP%%)) Note: The pipe symbol (|) is used in LDAP filter strings as an OR operator.
Email Attribute	Enter the name of the attribute that identifies the user's email address in the LDAP database. Applies only if you are using **user-based LDAP routing.**
Mailhost Attribute	Enter the name of the attribute that identifies the user's next-hop SMTP gateway on the LDAP server. Applies only if you are using **user-based LDAP routing.** If group-based routing is being configured, this field must be completed on the Policy Manager > Group > LDAP screen. The attribute will exist in each group entry (not in the user entries as in user-based routing) and will contain the next-hop SMTP server for all the group members.

Internal Routing

Administrators must provide the IP addresses of any internal server allowed to deliver, through IronMail, messages to external domains. The *IP address* of the default mail server (entered during the Initial Configuration Wizard when IronMail was installed) is listed by default. Whenever a server's IP address is added here, it is automatically added to IronMail's Allow Relay List (*Mail-Firewall > Allow Relay*). Note, however, that if an IP address in this table is deleted or edited, the Allow Relay List must be manually updated to reflect the change.


Inbound Routing List
Provide the IP addresses for any internal servers that will route messages to external domains. Whenever you add a server's IP address here, it is automatically added to the Allow Relay List (Mail Firewall > Allow Relay). If you edit or delete an IP address in this table, you must manually update the Allow Relay List to reflect the change.
IP Address
Side Note
Delete
10.50.1.53
Add an IP:
Side Note for IP:
Submit
Reset

Field	Description
Table Headers	The table at the top of the screen displays information about the internal servers that will route messages to external domains. The information includes: • IP Address - lists the IP addresses of the servers • Side Note - shows any explanatory text associated with the specific server • Delete - checkboxes (or a hyperlink) that allow deleting any or all IP addresses from the list.
Add an IP:	Enter the IP address of the server you wish to add
Side Note for IP:	Eenter an explanatory comment for the IP address added. Text longer than 255 characters is truncated.

Click "Submit" when the information has been entered correctly.

The Virtual Private Network

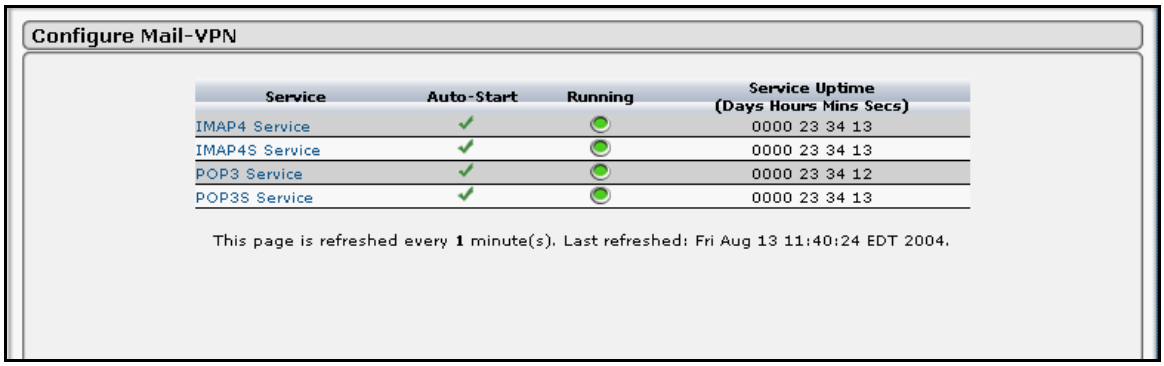
Configure Mail-VPN

Configure IronMail's services for processing message retrieval requests (via *POP3* and *IMAP4* protocols) in the Mail-VPN program area. When IronMail proxies these connections, the internal mail servers are protected from attempted attacks on these ports, as well as shielded from view to the outside world. When users retrieve their email, IronMail intercepts the requests, proxying them to the internal mail server(s). It passes the username and password to the internal mail server which is responsible for validating the request. If validated, IronMail proxies the internal mail servers' response back to the client.

Four IronMail subsystems are used to process these email connections.

- The **IMAP4 Service** listens for and processes email connections on the non-secure port 143 using the IMAP4 *protocol*.
- The **IMAP4S Service** listens for and processes connections on the secure port 993 using the IMAP4S protocol. (The "S" in the service's name represents "secure.")
- The **POP3 Service** listens for and processes connections on the non-secure port 110 using the POP3 protocol.
- The **POP3S Service** listens for and processes connections on the secure port 995 using the POP3s protocol. (The "S" in the service's name represents "secure.")

The Configure Mail-VPN table in the Mail-VPN page contains four columns: Service, Auto-Start, Running, and Service Uptime.

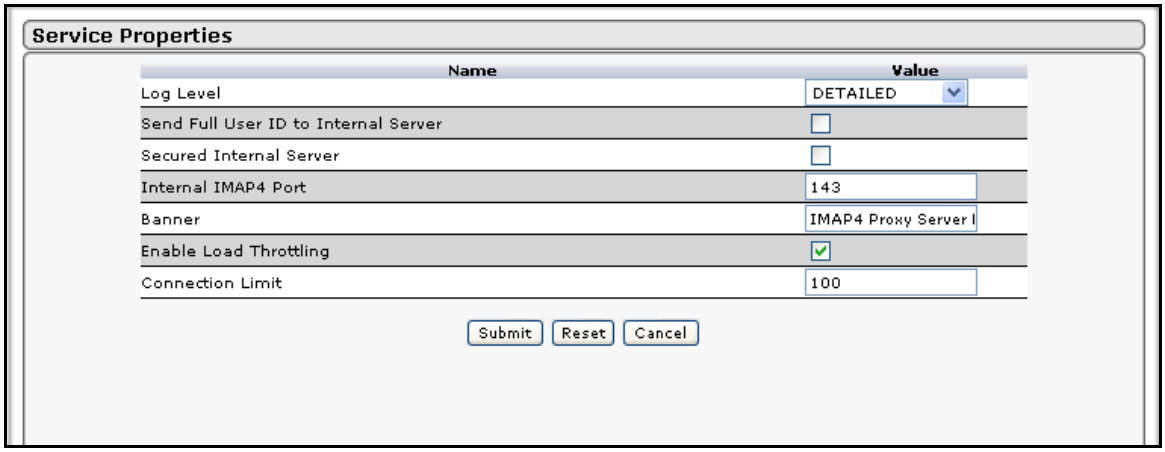


Field	Description
Service	This column contains the names of the IronMail Services or subsystems that process email retrieval requests.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If the icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green IronMail's *Health Monitor* will restart a Service that has stopped for any reason when it performs its tests on all appliance subsystems. If the icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off. A service cannot automatically start running, however, until its auto-start setting is turned on. Nevertheless, an adminstrator can manually start a service even when auto-start is disabled.) The red and green icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from an X to a check. If the icon does not toggle as expected, click the Configure Mail-VPN Services hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped by an administrator or by an unexpected program error, but was restarted automatically by IronMail's Health Monitor.

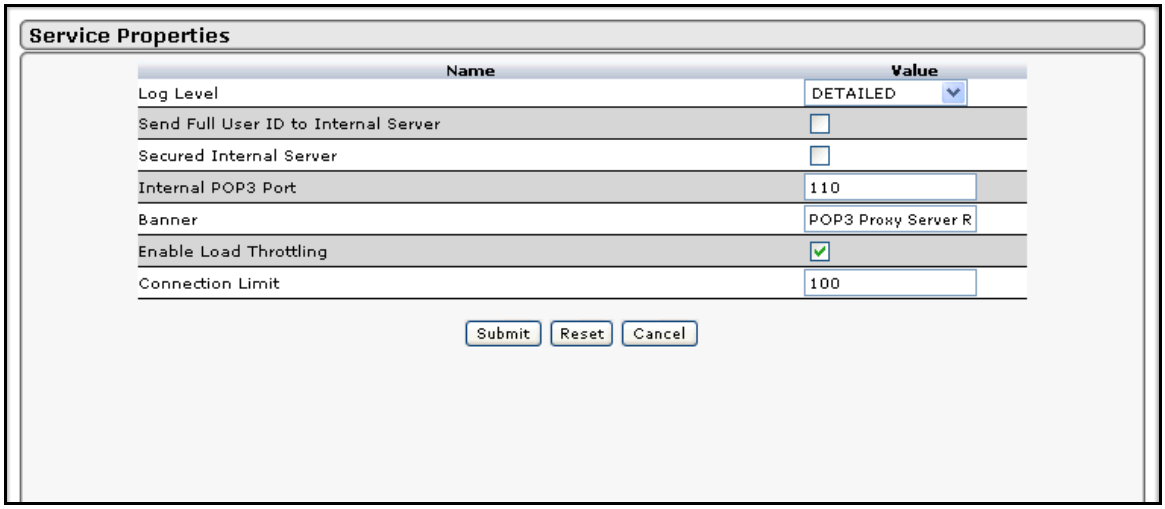
Each Service name is also a hyperlink that opens a secondary browser window in which configuration options for that Service are set.

IMAP4 and POP3 Services

The secondary Properties window for the *IMAP4*, IMAP4S, *POP3* and POP3S Services are identical, offering the following configuration options:



IMAP4 Properties



POP3 Properties

Field	Description
Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the amount of detail written to the log. Enter a value from 1 to 6, with 6 generating the most detail about the services' processing.

Send Full User ID to Internal Server	Internal email applications (e.g., Lotus Notes, Microsoft Exchange, and Novel GroupWise) may be configured to require users' client applications to submit a fully qualified username (e.g., username@domain.com). If "Send Full User ID to Internal Server" is enabled, IronMail will proxy the fully qualified username (and password) to the mail server. If not enabled, IronMail will only pass on the username part of a fully qualified user ID to the mail server. Users who belong to the Default Domain (specified in *Mail-Firewall > Configure Mail Services > Global > "Global Properties"*) may use a non-qualified username in their client application because the default mail server "knows them." However, a fully qualified username is required when IronMail hosts more than one domain—IronMail needs the domain-part of the fully qualified username to proxy a request to the proper internal mail server. (End users accordingly must configure their email clients accordingly with their fully qualified username in cases where IronMail proxies multiple domains.)
Secured Internal Server	In Step 9 page of the Initial Configuration Wizard, a "Mail Server Secure IMAP4/POP3 Enabled" option allows indication of whether or not the IMAP4/POP3 server supports secure (*SSL*) communications. (Note: Besides a security certificate, the capability must typically be enabled.) If that option was enabled, this "Secured Internal Server" option is enabled by default, indicating that IronMail should request a secure SSL session with the internal IMAP4/POP3 server. A secure connection is requested, not required. This option may be disabled at any time. Or if a Security Certificate is later installed on the internal IMAP4/POP3 server(s), this option may then be enabled.
Internal IMAP4/POP3 Port	Specify the port number through which IronMail should connect to the internal IMAP4/POP3 server. • The standard port number for IMAP4 is 143. • The standard port for IMAP4S is 993. • The standard port number for POP3 is 110. • The standard port number for POP3S is 995.
Banner	In order to hide information about the email infrastructure that might be exploited by hackers, IronMail provides the ability to create a neutral, nondescript Welcome Banner replacing the internal mail server's banner that might reveal its application-type and version. The banner is limited to 80 bytes of data, and may not contain new line feed characters (<CR>).
Enable Load Throttling	If "Enable Load Throttling" is selected, IronMail will allow a maximum number of simultaneous IMAP4/IMAP4S/POP3/POP3S connections. If this option is not enabled, IronMail will accept an unlimited number of simultaneous connections. Whereas SMTPI/SMTPIS load throttling is dynamic, gracefully adjusting connection acceptance-rate with the volume of messages in IronMail's Message Store, this IMAP4/IMAP4S/POP3/POP3S load throttling simply places a flat limit on the number of simultaneous connections these subsystems will each accept. If enabled, a numeric value must be provided in the input field appearing immediately below.
Connection Limit	Enter a number, from 100 to 200, representing the maximum number of simultaneous connections IronMail allows on each port. (Administrators may wish to monitor their daily volume of email for one or more weeks before setting this value. Review the corporate *firewall* Connection Log for ports 110, 143, 993 and 995 to determine what typical simultaneous connection rates are.)

Log Level Warning

Administrators must use their judgment in balancing the trade-off between detailed logs that assist in troubleshooting problems, and the enormity of the file size that might result. In a high mail-volume environment (50,000+ messages a day), it is not unusual for the daily SMTPI log to be 100 MB or more. If administrators choose to set the logging level to "Detailed," they are strongly advised to set IronMail's Cleanup Schedule (*System > Cleanup Schedule*) to delete log files after they are three days old.

Detecting Intrusions

Mail-IDS

The Mail-IDS (Intrusion Detection System) program area provides a variety of tools designed to detect *network* attacks against the email gateway, as well as a tool to test for weaknesses or vulnerabilities in specific internal mail servers. IronMail will automatically generate alerts for certain types of network attacks, notifying administrators immediately by email, pager, or SNMP that an event has occurred. For all attack events, IronMail will log their occurrence so they may be viewed in IronMail's log files and daily reports, and in IronMail's Dashboard. Administrators, therefore, should configure IronMail's Alert Manager (*Monitoring > Alert Manager*) to send to them alerts that the Mail-IDS services generate. And administrators should routinely monitor IronMail's Dashboard and Mail-IDS Report throughout each day.

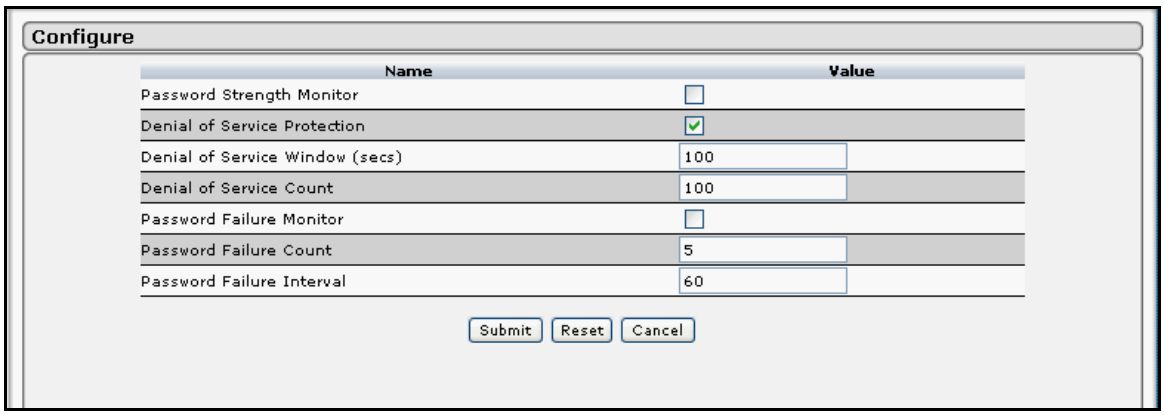
Use the Application Level, Network Level, System Level, Anomaly Detection, and Vulnerability Assessment hyperlinks in the left navigation frame to navigate to the specific Mail-IDS tools.

Application Level Protection

IronMail offers tools designed to protect against attacks directed at email applications. The Application hyperlink in the left navigation frame expands to offer DoS (Denial of Service), Password Strength, Password Cracking, and Configure sub-menus.

Configure Application Level Protection

Use the values entered in this window to set the threshold for application-level attacks aimed at the internal network.



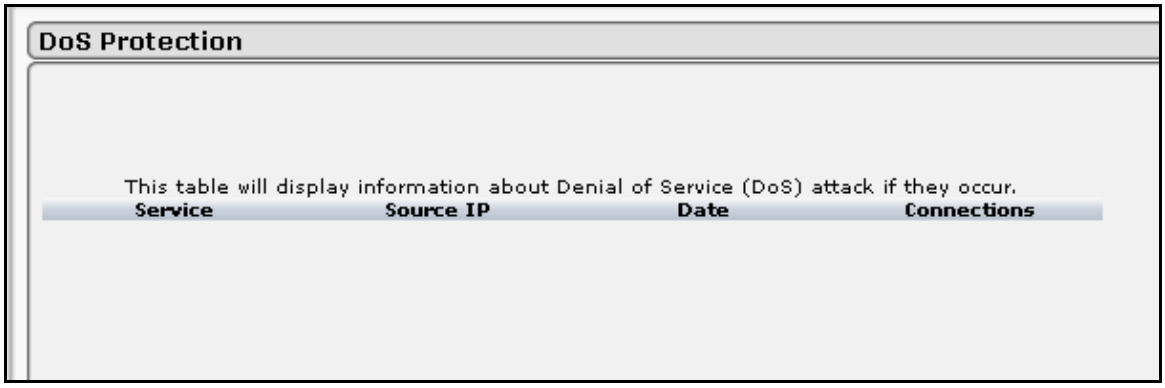
The Configure Application Level Protection Table requests the following information:

Password Strength Monitor	If enabled, IronMail will pass all passwords, submitted by end users' mail clients as they retrieve their email, through an algorithm that measures their relative "strength." The algorithm checks for length, use of upper and lower case, and alphanumeric characters, and the equivalency between the password and username and administrator-defined "keywords." Passwords are "parsed" in memory and are not saved to disk. Users' "password strength" may be viewed at *Mail-IDS > Application Level > Password Strength*. Additionally, the daily Mail-IDS Report reports password strength information (*Monitoring > Reports/Log Files > Reports > "Mail-IDS"*).
Denial of Service Protection Be aware that in some environments, applications legitimately make high numbers of connections which IronMail may interpret as a Denial of Service attack. Consult with the *network* administrator before setting this value.	If Denial of Service Protection is enabled, IronMail will monitor all TCP connections to all email ports on which it listens (25, 110, 143, etc.), and block future connections for any *IP address* that exceeds the Denial of Service threshold (created with the two values that appear immediately below). IronMail will discontinue accepting connections from the offending IP address for the length of time specified in the "Denial of Service Window" below. Once that length of time passes, IronMail will again begin allowing connections from that source IP address. Ensure that IronMail's Alert Manager (*Monitoring > Alert Manager*) is configured to send Warning alerts for the *POP3*, *IMAP4*, and SMTPI Services so an administrator may immediately add the offending IP address to IronMail's Local Deny List (*Anti-Spam > Deny List > Local Deny List*), after which IronMail will no longer accept connections from that IP address.
Denial of Service Window	Enter a number, from 1 to 65,535, representing the length of time in seconds in which connections from a single IP address will be accepted after which a Denial of Service attack is assumed. (The default value of "100" is generally acceptable.) If IronMail receives the number of connections specified in the "Count" field above within this "window," further connections from the source IP address will be dropped. IronMail also uses this value as the length of time IronMail rejects further connections. Once the time has lapsed, IronMail again begins accepting connections from the source IP address.
Denial of Service Count	Enter a number, from 1 to 65,535, representing the maximum number of allowed connections to a single port before which a Denial of Service attack is assumed. (The default value of "100" is generally an acceptable value.) When a single IP address generates the specified number of connections within the time frame indicated below, a Denial of Service attack is assumed and further connections from that source will be dropped.
Password Failure Monitor	Enter a number, from 1 to 65,535, representing the maximum number of allowed connections to a single port before which a Denial of Service attack is assumed. (The default value of "100" is generally an acceptable value.) When a single IP address generates the specified number of connections within the time frame indicated below, a Denial of Service attack is assumed and further connections from that source will be dropped.
Password Count	If a user enters an invalid password/username the number of times specified here, within the time frame indicated below, IronMail assumes someone is attempting to crack a user's password. Enter a number between 1 and 100.

Password Failure Interval	Enter a number, from 1 to 65,535, representing the maximum number of allowed connections to a single port before which a Denial of Service attack is assumed. (The default value of "100" is generally an acceptable value.) When a single IP address generates the specified number of connections within the time frame indicated below, a Denial of Service attack is assumed and further connections from that source will be dropped.

Denial of Service Protection

IronMail automatically monitors and logs repeated connections to a specific port from the same *IP address*. If an administrator-defined number of connections to a single port are attempted within a specified period of time, IronMail assumes that it is a Denial of Service (DoS) attack and will drop all incoming connections to that port from that address for a user-specified amount of time. The Denial of Service threshold (a specified number of connections within a defined length of time) is set in Mail-IDS > Application Level > Configure > "Denial of Service Count" and "Denial of Service Window."



The Denial of Service Protection and Monitoring table lists a summary of all DoS attacks recorded since IronMail's cleanup process deleted the DoS data (see *System > Cleanup Schedule*); each time this page is refreshed, the data is updated with the most recent attacks. The information here may also be viewed in the daily Mail-IDS Report created at approximately midnight each day (*Monitoring > Reports/Log Files > Reports > "Mail-IDS "*). Note, however, that whereas IronMail's Denial of Service window may show several days' (or more) worth of information, the daily Mail-IDS report will only show 24 hours worth of data.)

Field	Description
Service	This column reports which of the IronMail services encountered the Denial of Service (DoS) attack: *POP3*/POP3S, *IMAP4*/IMAP4S, or SMTPI/SMTPIS.
Source IP	This column reports the IP address from which the DoS attack originated. Consider adding the IP address to IronMail's Local Deny List (*Anti-Spam > Deny Lists > Local Deny List*) to block all further SMTP connections from that source.
Date	This column reports the timestamp when the DoS threshold was reached. If the same IP address generates another DoS later in the day, the previous timestamp is updated to reflect the time of the new attack.

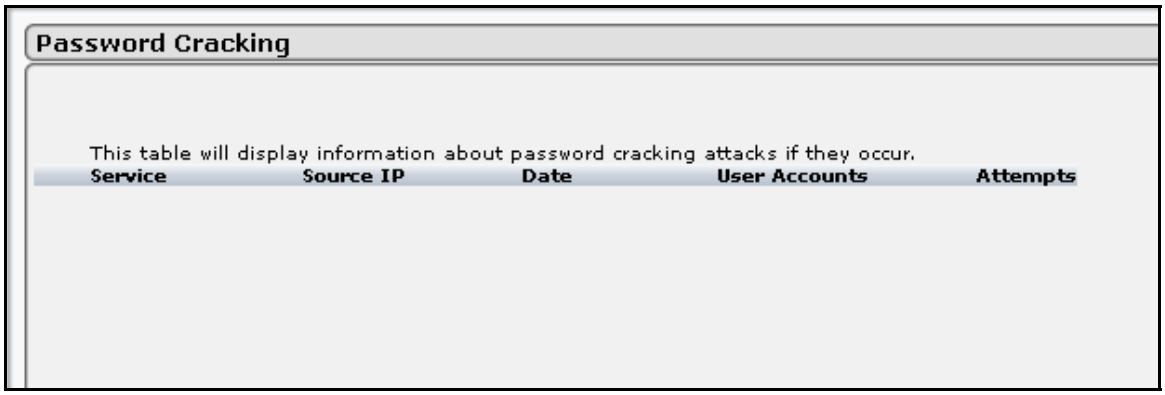
Connections	This column reports the number of connections that were dropped after the DoS threshold was reached. Remember that IronMail will drop further connections only for the length of time specified as the "Denial of Service Window." If multiple DoS attacks from the same IP address are detected throughout the day, IronMail will display in this column a running total of dropped connections that occurred during the separate "drop windows" that follow each time a threshold was reached.

Do not confuse the Denial of Service threshold with the SMTPI, POP3, and IMAP4 "Load Throttling" thresholds. This Denial of Service threshold occurs at the *Network* layer, whereas Load Throttling occurs at the Application Level.

Note that when an IP address is placed on IronMail's Allow Relay list (*Mail-Firewall > Allow Relay*), it will not be evaluated for Denial of Service attacks. This may be a potential vulnerability.

Password Cracking

If "Password Failure Monitor" is enabled (*Mail-IDS > Configure > "Password Failure Monitor"*), IronMail will log every instance that a failed logon threshold has been reached. (Administrators establish the threshold in Mail-IDS > Configure > "Password Failure Count" and "Password Failure Interval.") Additionally, if the number of failed logon attempts reaches the threshold, IronMail can generate an email, pager, or SNMP alert to the administrator. This on-screen display of Password Cracking lists a cumulative summary of threshold-level failed logons since IronMail's last cleanup deleted old data (*System > Cleanup Schedule > "IDS Statistics"*); the data is updated each time this page is refreshed. (The daily Mail-IDS Report on Password Cracking begins anew each day at midnight, and displays only the previous 24 hours worth of data.)



The Password Cracking table displays:

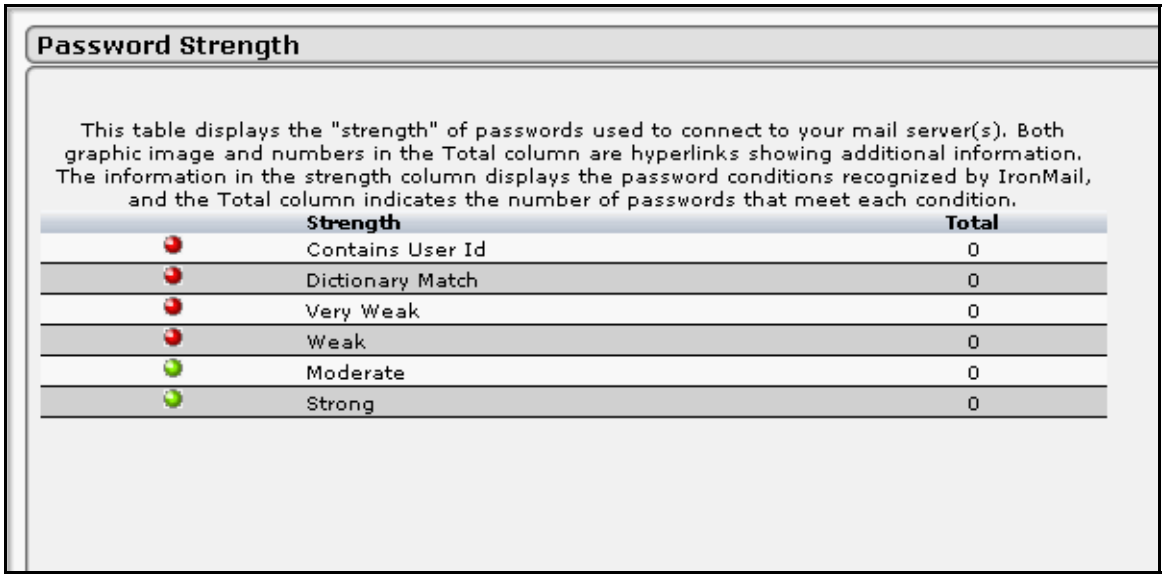
Field	Description
Service	This column reports which of the IronMail services encountered the Password Cracking attempt: *POP3* or *IMAP4*.
Source IP	This column reports the *IP address* where the attempted logon originated.
Date	This column reports the timestamp when the Password Cracking threshold was reached.
User Accounts	This column reports the username used for the attempted logon.

Attempts	This column reports a cumulative total of failed attempts, including the failed attempts prior to the threshold being reached. For example, if the threshold was "10" and was reached at 10 AM in the morning, but a hacker made 75 additional password cracking attempts, during the day, The Password Cracking table would report 85 attempts at the end of the day.

Administrators are encouraged to configure the Alert Manager to send Information alerts for the POP3 and IMAP4 Services which generate the Password Cracking alerts. (See Alert Manager.) Once an alert has been received, the administrator may add the source IP address to IronMail's Local Deny List (Anti-Spam > Deny List > Local Deny List).

Password Strength

If "Password Strength Monitor" is enabled (Mail-IDS > Configure > "Password Strength Monitor"), passwords are analyzed as IronMail's *POP3* and *IMAP4* Services proxy username and password to the internal mail server. IronMail does not "store" or save the password to disk—rather, it analyzes the text strings in memory "on the fly." IronMail uses an algorithm that tests each password's relative "strength," displaying its results in the Password Strength Monitor table on this page. The table shows a cumulative summary of all passwords checked since IronMail's last cleanup deleted old data (*System > Cleanup Schedule > "IDS Statistics*"). The data on this page is updated each time the page is refreshed.


Password Strength
This table displays the "strength" of passwords used to connect to your mail server(s). Both graphic image and numbers in the Total column are hyperlinks showing additional information. The information in the strength column displays the password conditions recognized by IronMail, and the Total column indicates the number of passwords that meet each condition.
Strength
Total
Contains User Id 0
Dictionary Match 0
Very Weak 0
Weak 0
Moderate 0
Strong 0

Strength IronMail's algorithm checks for the following password characteristics:

- Password contains the individual's User ID or username.
- Password matches a word in a user-defined word list. Is there still a user-defined list? How is it accessed?
- Very weak: less than 8 characters, and either all alpha or all numeric.
- Weak: 8 or more characters, and either all alpha or all numeric.
- Moderate: between 5 to 7 characters and combination of alpha and numeric.
- Strong: 8 or more characters and combination of alpha, numeric, and special characters.

The **Total** column displays how many users have passwords at each level of "strength."

Network Level Protection

IronMail provides a *Network* IDS engine that examines in real-time all network traffic flowing through email ports (ports 25, 110, 465, etc.). Viewable through IronMail's Analysis Console, it begins creating a log whenever data or network packets match known "signatures" for attempts at hacking. Once detected, the entire stream of packets is captured for analysis.

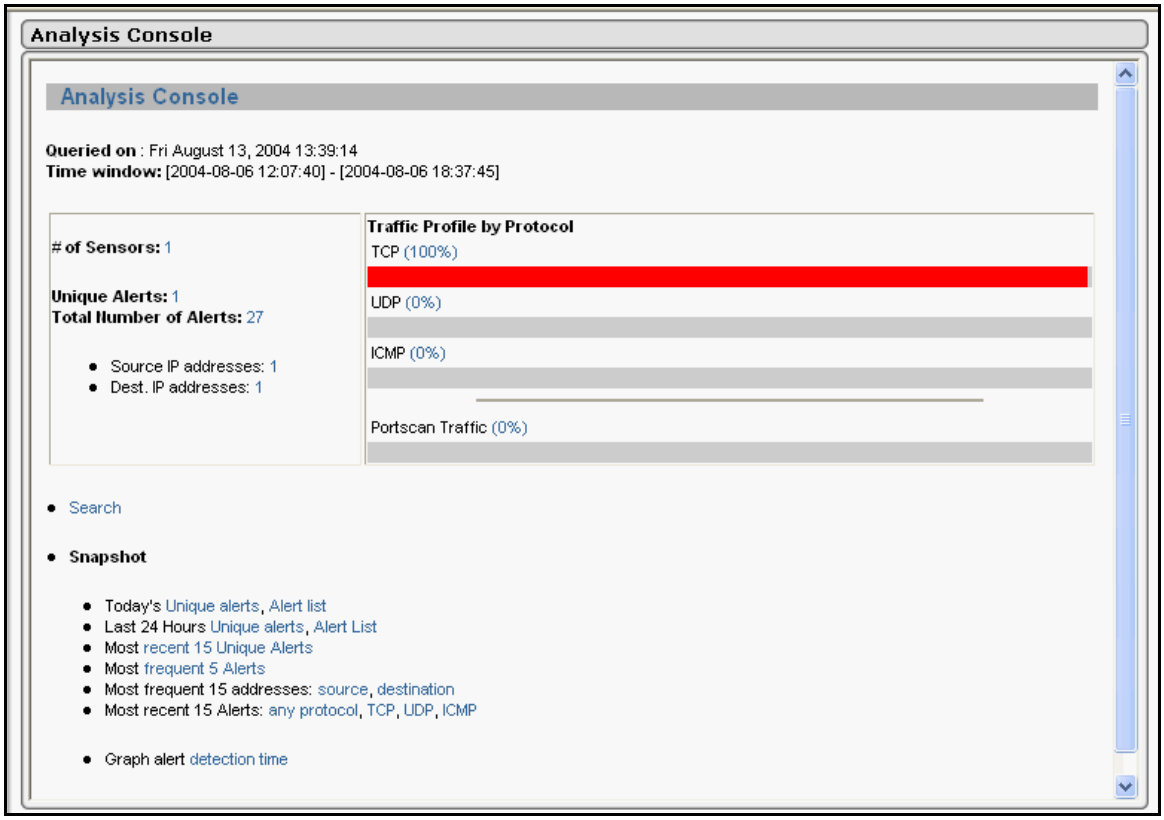
For those administrators who actively respond to network attacks and create rules to block future occurrences, the Analysis Console provides visibility into network traffic at the TCP level. It is assumed that users taking advantage of this tool are already experienced and knowledgeable in its use.

The Network Level hyperlink in the left navigation frame expands to offer Analysis Console, Configure, and Signature Manager sub-menus.

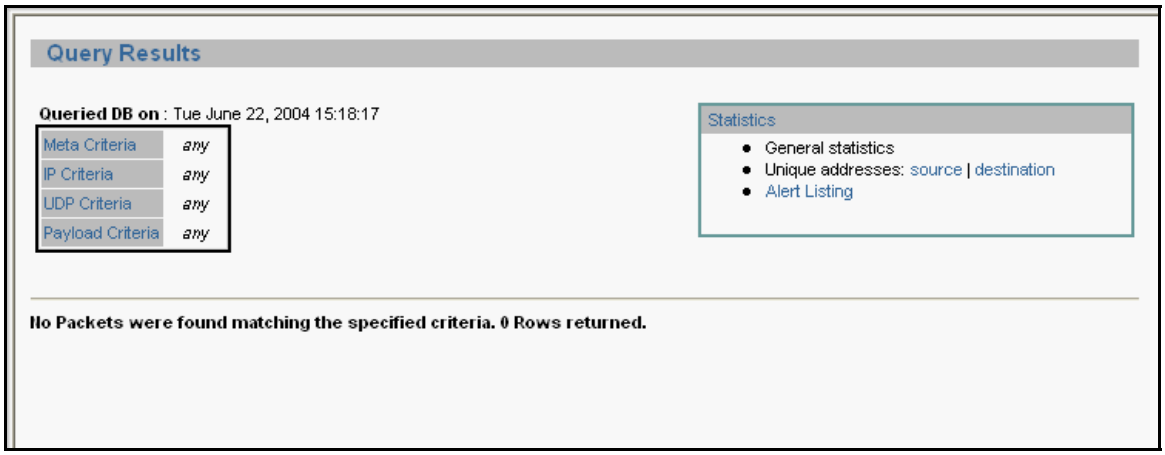
Analysis Console

The Analysis Console displays a static report—information captured up to the moment the Analysis Console was opened. Re-clicking the Analysis Console hyperlink in the left navigation frame refreshes the report with the latest information.

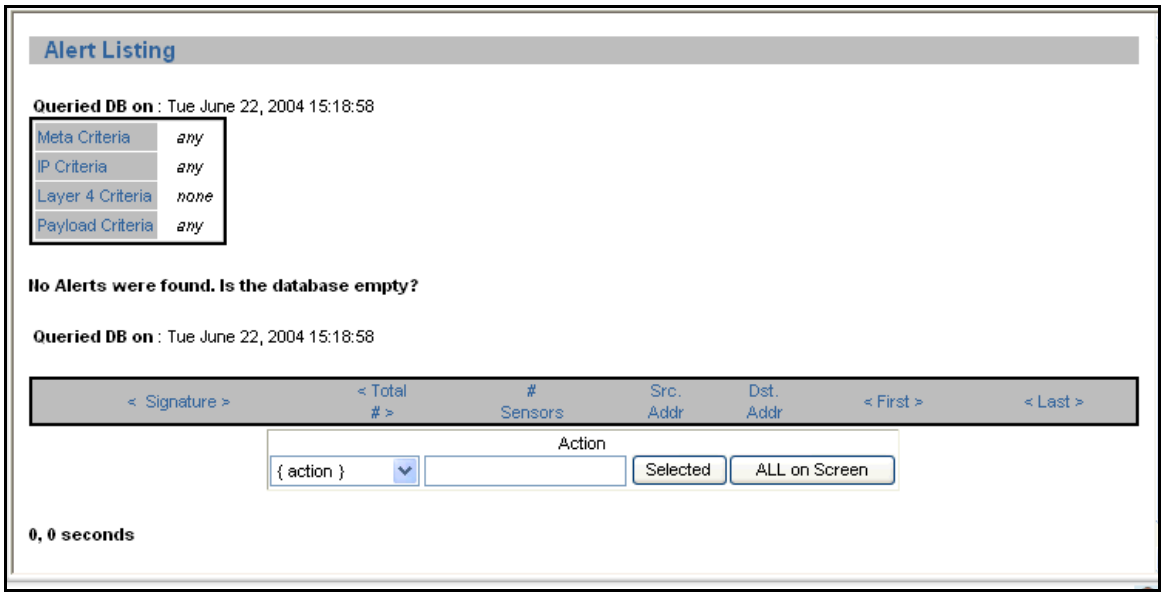
The Analysis Console reports "Alerts"—instances of TCP, UDP, and IMCP traffic that matched an attack signature for which *Network* IDS was scanning. Network IDS uses the attack signatures specified in *Network Level > Signature Manager* to identify these attacks.


Analysis Console
Analysis Console
Queried on : Fri August 13, 2004 13:39:14
Time window: [2004-08-06 12:07:40] - [2004-08-06 18:37:45]
# of Sensors: 1
Unique Alerts: 1
Total Number of Alerts: 27
Source IP addresses: 1
Dest. IP addresses: 1
Traffic Profile by Protocol
TCP (100%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)
Search
Snapshot
Today's Unique alerts, Alert list
Last 24 Hours Unique alerts, Alert List
Most recent 15 Unique Alerts
Most frequent 5 Alerts
Most frequent 15 addresses: source, destination
Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
Graph alert detection time

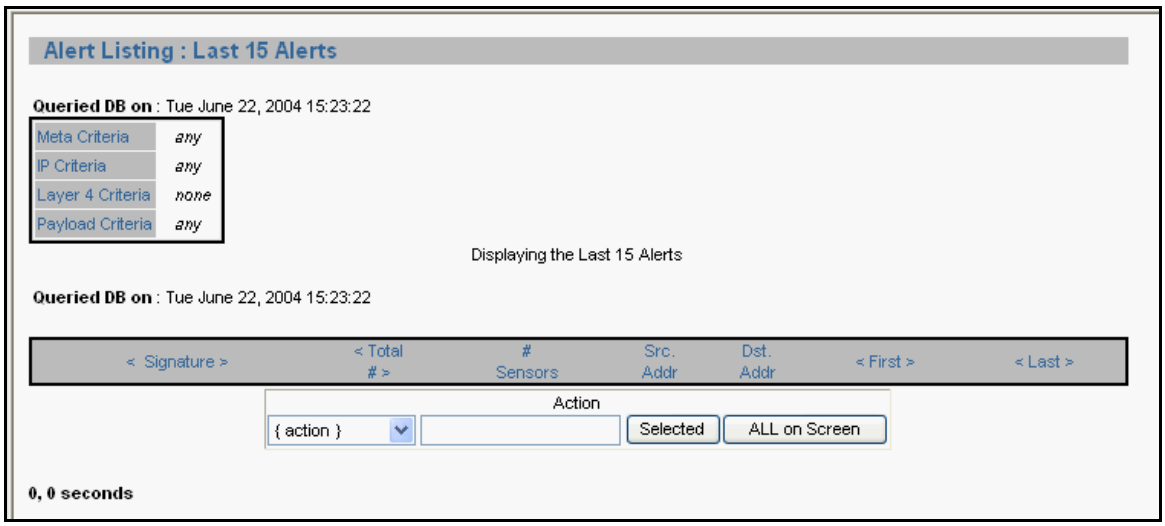
Text appearing in blue is a hyperlink to additional information about each event. Clicking the "TCP" percentage hyperlink, for example, shows a list of all TCP attacks detected in a refreshed window.


Query Results
Queried DB on : Tue June 22, 2004 15:18:17
Meta Criteria any
IP Criteria any
UDP Criteria any
Payload Criteria any
Statistics
General statistics
Unique addresses: source | destination
Alert Listing
No Packets were found matching the specified criteria. 0 Rows returned.

Other examples are shown below.



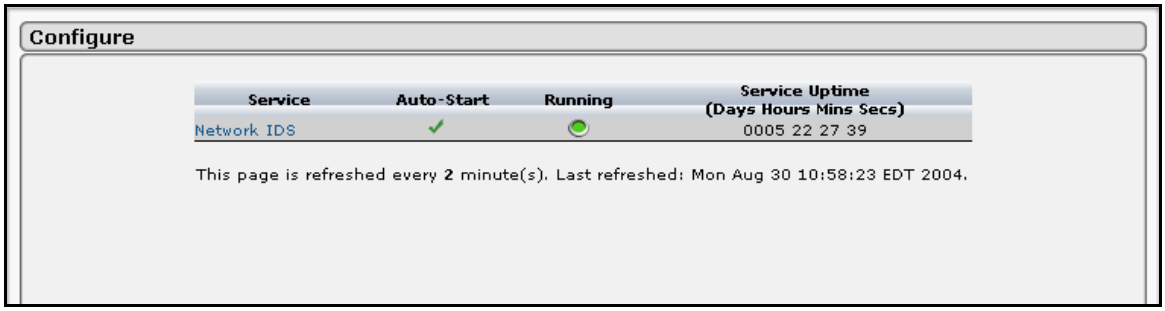
Query Results for Total Number of Alerts



Query Results for Last 15 Alerts

Configure Analysis Console

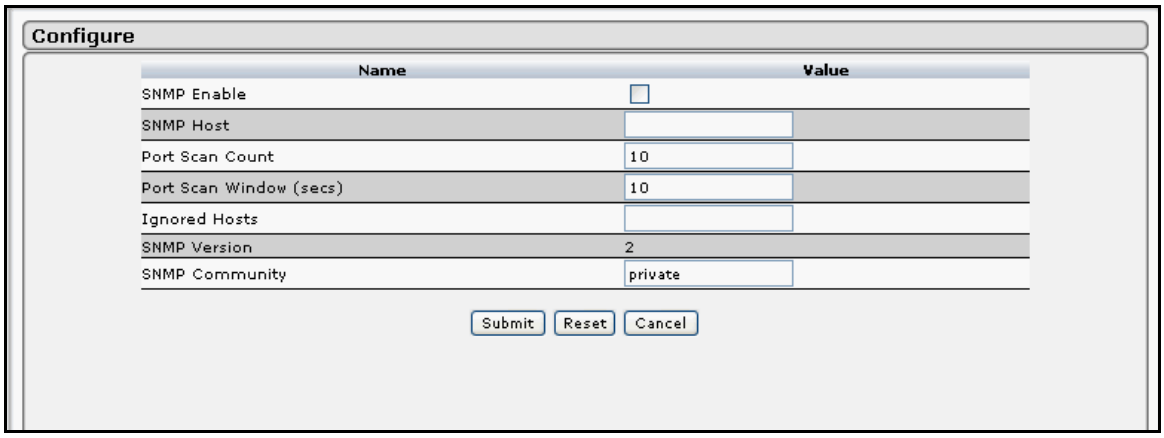
The Analysis Console is disabled by default.



Click the red X in the Auto-Start column to start the Analysis Console automatically when IronMail restarts. (The red X turns into a green check.) Click the "running" icon (red when currently stopped—green when currently running) to start or stop the Analysis Console.

Field	Description
Service	"Network IDS" in the Service column is a hyperlink opening a secondary property window allowing configuration of this service.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If an icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green, the service will restart when IronMail's Health Monitor performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off. A service cannot start running, however, until its auto-start setting is turned on.) The red and green light icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the Running icon may not refresh, i.e. change from green to red, as expected. If the icon does not toggle, click the Configure hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the Running icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped by an administrator or unexpected program error, but was restarted automatically by IronMail's Health Monitor.

Clicking the *Network* IDS hyperlink opens a secondary browser window allowing configuration of the Network IDS Service.



The following configuration options are available:

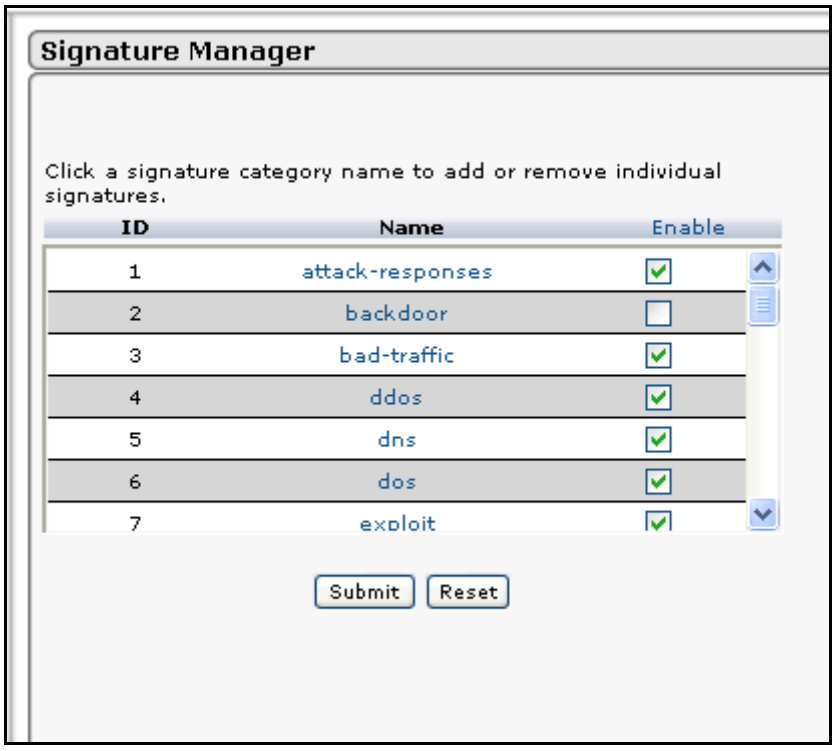
Field	Description
SNMP Enable	Select the **SNMP Enable** check box to allow IronMail's Analysis Console to deliver its network events as traps to a network SNMP console. Note that enabling SNMP here is independent of enabling SNMP in IronMail's Alert Manager. That is, enabling SNMP traps as an alert mechanism for IronMail's alerts does not automatically allow the delivery of Analysis Console traps.
SNMP Host	Enter the hostname of the SNMP server.
Port Scan Count	Whereas the Denial of Service configuration (*Mail IDS > Application Level > Configure > "Denial of Service Count" and "Denial of Service Window"*) establishes a threshold for connections from a single *IP address*, that threshold is specific to TCP connections to a single port. This Port Scan threshold counts any TCP connection to any port that originates from the same IP address. Enter a maximum number of allowed connections, from 1 to 65,535, in the "Count" field. When a single IP address generates the specified number of connections within the time frame indicated below, the connection will be logged as an Analysis Console "event." In addition to detecting TCP connections, Analysis Console detects stealth scans (precursor or reconnaissance activity prior to an attack). A single instance of a NULL, FIN, SYNFIN, or XMAS-type stealth scan will be logged as an Analysis Console "event."
Port Scan Window (secs)	Enter a number of seconds, from 1 to 65,535, in the "Port Scan Window" field indicating the "window" in which connections may occur. When a single IP address generates the specified number of connections within the time frame indicated here, the connection will be logged as an Analysis Console "event."
Ignored Hosts	Enter the IP address for any host IronMail should ignore. (These hosts are allowed to scan IronMail as much and as often as they like.) Use commas to separate multiple IP addresses from each other.
SNMP Version	Enter the SNMP version number. Note that IronMail only supports SNMP version 2c. When entering the SNMP version number in this input field, however, only enter the numeral "2."
SNMP Community	By default, when SNMP is installed, two default "communities" are created: "Private" and "Public." The SNMP administrators should have created one or more idiosyncratic community names for the services SNMP is monitoring. Enter that community name in this input field.

Click **Submit** to save the values. Click **Close** to close the window.

Note that if the Analysis Console is enabled, administrators should monitor the number of generated events on a regular basis—one or more times a day if necessary. High numbers of events stored in IronMail's database can begin to adversely affect overall IronMail performance. If more than 100,000 IDS events are recorded and stored to disk before IronMail's Cleanup Schedule deletes old Mail-IDS data files, lower the "age" at which IronMail should delete data. That is, if IronMail's Cleanup Schedule is configured to wake up every 24 hours and delete files that are 48 hours old, consider re-configuring it to wake up every 12 hours and delete data that is 24 hours old.

Signature Manager

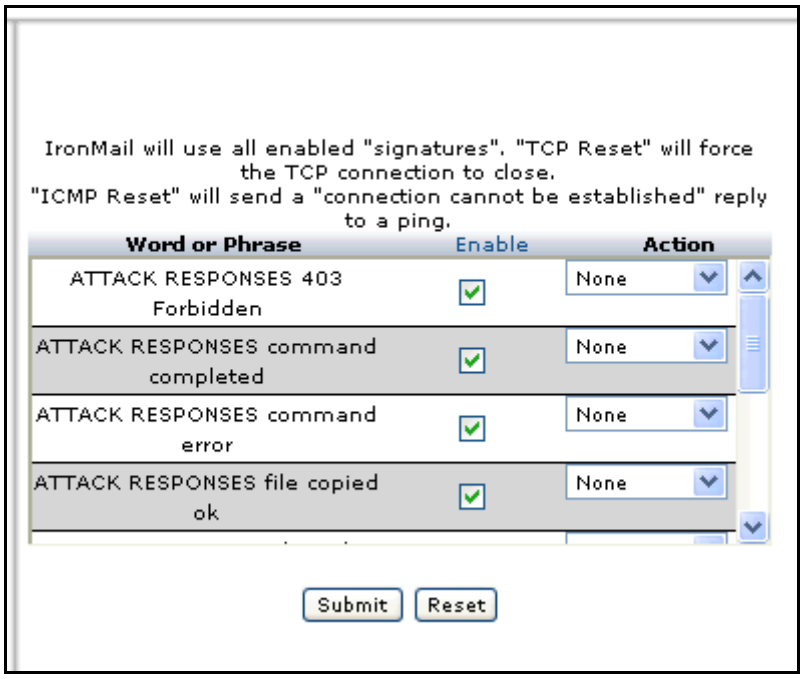
The Network IDS Service compares *packet* information against over 1300 known attack signatures. The Signature Manager table displays a list of broad categories of attack threats.



The table displays:

Field	Description
ID	This column indicates the ID number, used internally by IronMail, of the category of attack signatures.
Name	This column displays the “category name” of a set of attack signatures. The category name is indicative of the type of attacks they identify. For example, “ddos” is a category containing signatures that identify a variety of distributed denial of service attacks, and “web-cgi” is a category of signatures related to attacks against web-based CGI applications and scripts. The category name is also a hyperlink that opens in a secondary browser window a list of all the individual signatures within that category.
Enable	The **Enable** check boxes for each category allow the administrator to decide whether or not to include an entire category of signatures in IronMail’s real-time analysis of email traffic.

Click an attack category's hyperlink to open, in a secondary browser window, a list all the individual attack signatures within that category.



The following information is displayed:

Field	Description
Word or Phrase	This column identifies a "friendly" name of the attack signature.
Enable	Select or deselect a signature's **Enable** check box to indicate whether or not IronMail should include it in its real-time analysis of email traffic.
Action	IronMail is capable of actively responding to some attacks, typically by resetting the TCP connection. If an action is possible, the Action column will display a pick list allowing the choice of either "TCP Reset" or "ICMP Reset." Leave the action set to "None" if IronMail should not reset the connection if an attack is detected. Only administrators familiar with *firewall* rules should enable actions for attack signatures. IronMail will blindly reset connections when it encounters packet data it thinks matches attack signatures, whether the data stream is valid or not. And because IronMail has been specifically "hardened," and thus immune from these attacks, setting an action may be moot.

Signature Updates

Note that CipherTrust regularly updates its database of attack signatures; updated signatures may be automatically downloaded and installed on individual IronMail's. However, customers must have purchased a Mail-IDS Updates license to benefit from these updates.

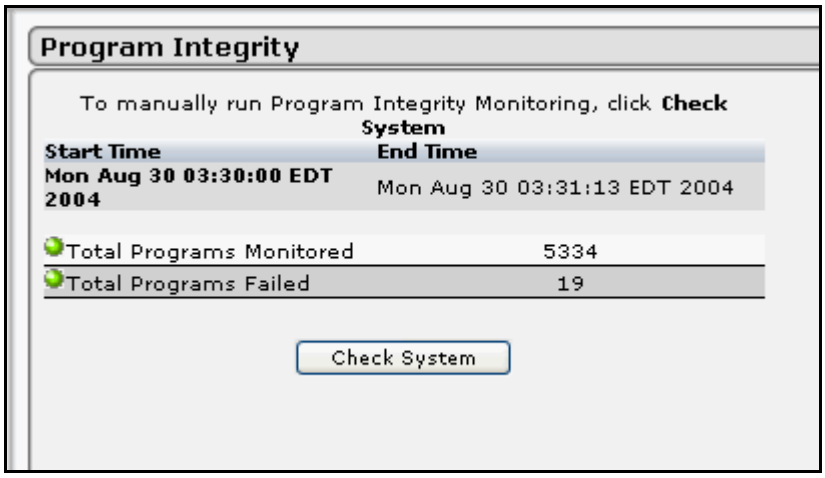
Protection at the System Level

IronMail is foremost an appliance to protect the internal mail servers sitting behind it. An integral component of its security, however, is ensuring that it (that is, IronMail) has not been compromised by an attacker. The Program Monitor and File Monitor services, therefore, check IronMail's program files and filesystem in order to detect whether or not an attempt has been made to alter code in any of its files, or if an attempt was made to insert Trojan horses or delete important system files. The first time IronMail restarts after the Initial Configuration Wizard is run, its Program Monitor and File Monitor test the system in order to build an initial database of IronMail's file set and file system. Thereafter, these two services run nightly, immediately before the Mail-IDS log is generated. Administrators may run File Monitor and Program Monitor "on demand" at any time by clicking **Check System** in their respective windows.

The System Level hyperlink in the left navigation frame expands to offer Program Integrity and Filesystem Integrity sub-menus.

Program Integrity

Every night, at approximately midnight, IronMail examines every executable file within its scope to verify that they have not been altered. The Program Integrity page displays how many files were scanned, and the number of files that failed its test, i.e. are now different from their original version. To manually run IronMail's Program Monitoring in-between scheduled sessions, click **Check System**. It will take a little less than a minute to run its tests.

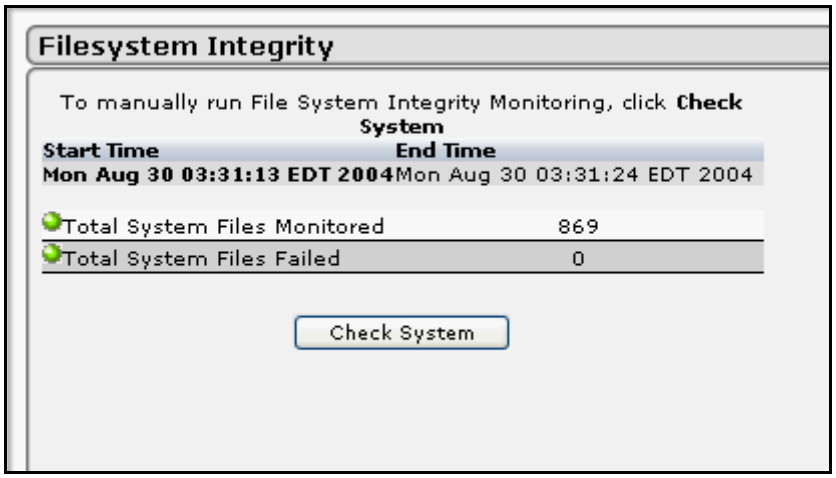


After clicking **Check System** IronMail will check, approximately every 10 seconds, if Program Integrity Monitor has finished its tests, then refresh the page with the results. If Program Integrity Monitor ever reports that a single file failed, contact CipherTrust Technical Support immediately. (Click the CipherTrust hyperlink at the bottom of any IronMail page to view contact information.)

The information available here may also be viewed in IronMail's Dashboard and the Mail-IDS Report that is created daily.

Filesystem Integrity

Similarly, every night at approximately midnight, IronMail examines its internal filesystem to ensure that no non-IronMail-generated files have been created on it or that none of IronMail's files were deleted. To manually run IronMail's File Monitoring in-between scheduled sessions, click **Check System**. It will take a little less than a minute to run its tests.



Approximately every 10 seconds, IronMail will check if Filesystem Integrity Monitor has finished its tests, and then refresh the page with the results. If Filesystem Integrity Monitor ever reports that a single file failed, contact CipherTrust Technical Support immediately. (Click the CipherTrust hyperlink at the bottom of any IronMail page to view contact information.)

The information available here may also be viewed in the Mail-IDS Report that is created daily.

Anomaly Detection

Anomaly Detection is a heuristic engine that examines patterns of email traffic in a *network*. It is "email message characteristic-aware"—that is, it recognizes when specific email characteristics have been seen in the network over a period of time. Administrators may configure the Anomaly Detection Engine (ADE) to issue alerts or create rules that act on future messages when specific patterns of email are detected.

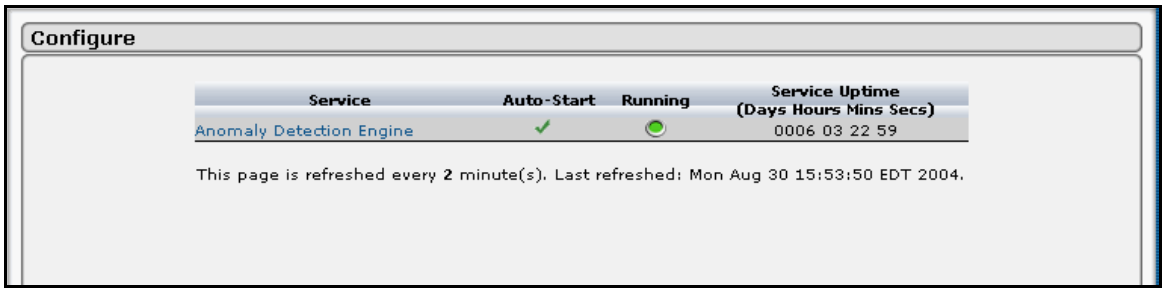
The heuristic is based on thresholds where "time," "frequency," and "email characteristics" converge. That is, if a specified number of emails with the defined characteristic(s) enter the network within the designated window of time, ADE can create a rule that takes an action on all future messages with that characteristic, or send an email notification to the administrator.

Anomaly Detection is an historical, not a real-time, analysis of events—it does not process messages like IronMail's Queue Services. That is, at an administrator-defined interval, it looks in IronMail's database that stores information about all the email it processed since it last ran its check. If a threshold was reached during the previous period of time, IronMail will either generate an alert message or create a *rule*, depending on the ADE's configuration.

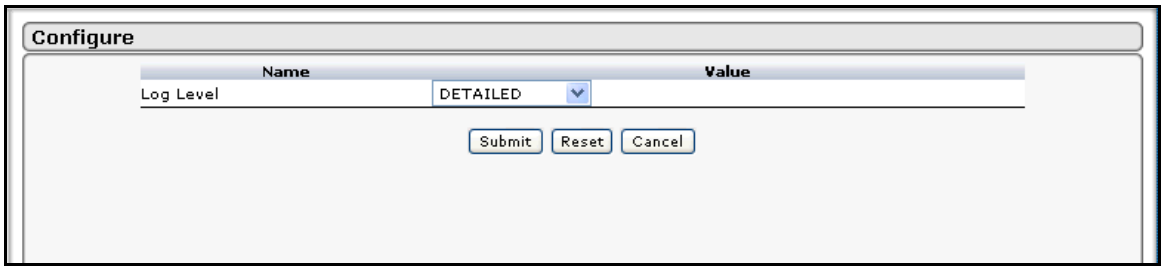
The Anomaly Detection hyperlink in the left navigation frame expands to offer Configure, Create Anomaly Rules, and Show Anomaly Rules sub-menus. Configure the ADE service parameters in the "Configure" page. Create anomaly detection queries, or rules, in the "Create Anomaly Rules" page, and view (and edit) the various queries within the "Show Anomaly Rules" page.

Configure Anomaly Detection

The Configure Anomaly Detection page allows the administrator to select start, stop, and auto-start options, as well as set a logging level for the service.

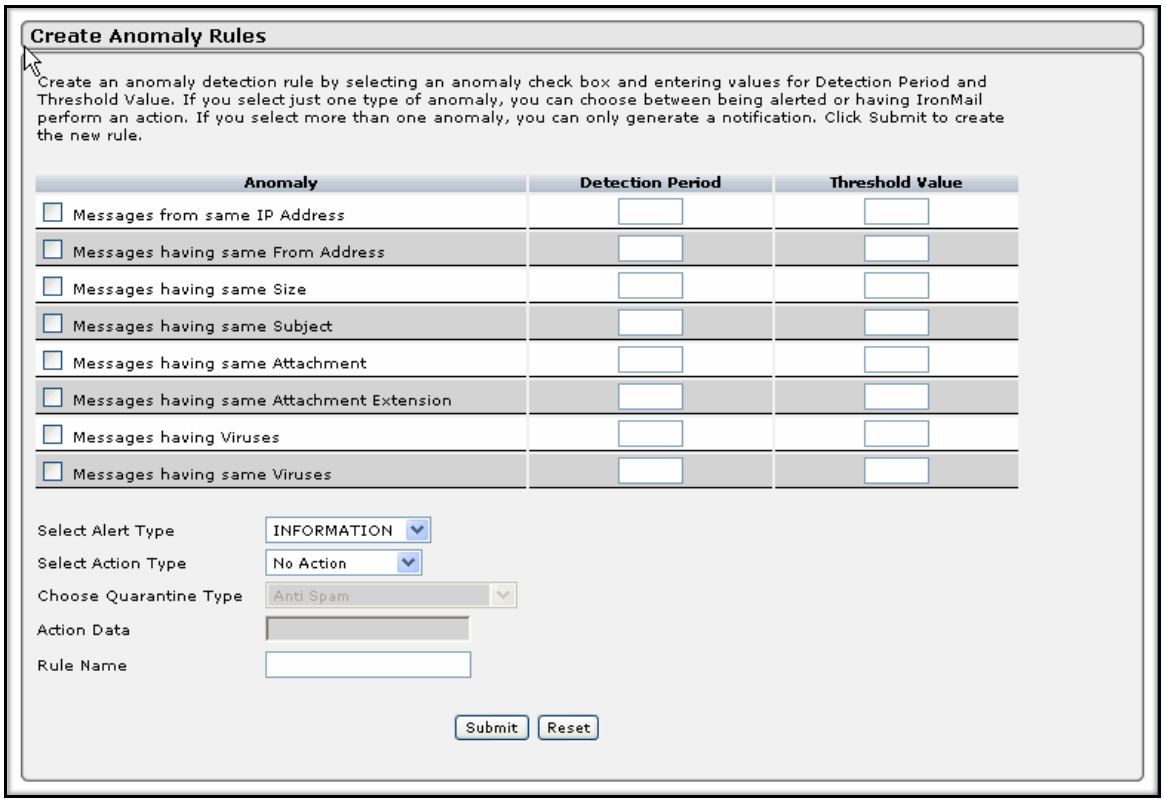

Configure
Service
Auto-Start
Running
Service Uptime (Days Hours Mins Secs)
Anomaly Detection Engine
0006 03 22 59
This page is refreshed every 2 minute(s). Last refreshed: Mon Aug 30 15:53:50 EDT 2004.

Field	Description
Service	This column identifies the Anomaly Detection Engine Service. The service name is also a hyperlink—a Properties page opens in a secondary browser window so that a logging level for the Anomaly Detection Engine may be set.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If the icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green, the service will restart when IronMail's Health Monitor performs its tests on all appliance subsystems. If the icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off. A service cannot start running, however, until its auto-start setting is turned on.) The red and green icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh, i.e. change from green to red, as expected. If the icon does not toggle, click the Configure Mail Services hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped by an administrator or by an unexpected program error, but was restarted automatically by IronMail's Health Monitor.



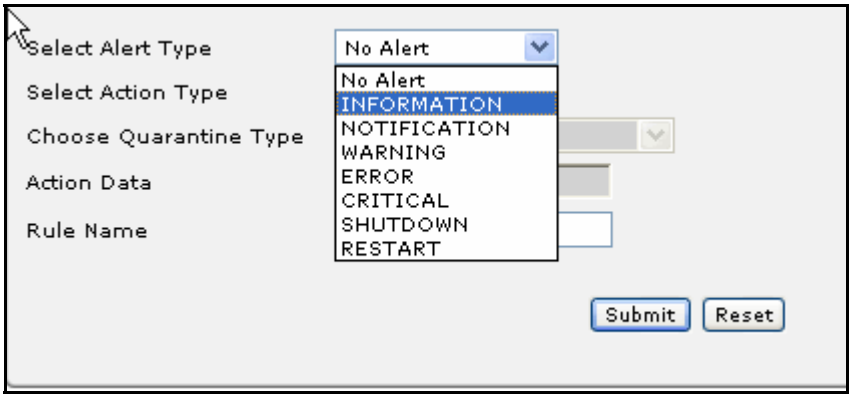
Create Anomaly Rules

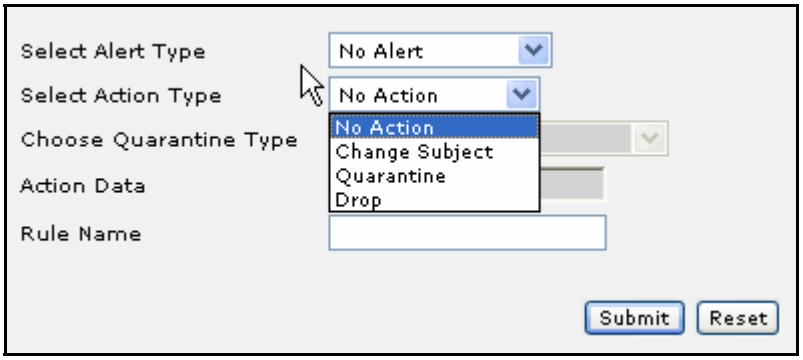
The rules created here are, in a sense, queries that look for and then respond to the types of email events identified in the table below. Queries based on some message characteristics are only capable of creating rules that generate alert messages. Queries based on other characteristics can create rules that take an action on future occurrences of a message-type. Also note that among the characteristics that allow actions, there is some variation: some allow the ability to Rename Subject Line, Quarantine, or Drop, while others only allow Drop actions.


Create Anomaly Rules
Create an anomaly detection rule by selecting an anomaly check box and entering values for Detection Period and Threshold Value. If you select just one type of anomaly, you can choose between being alerted or having IronMail perform an action. If you select more than one anomaly, you can only generate a notification. Click Submit to create the new rule.
Anomaly
Detection Period
Threshold Value
Messages from same IP Address
Messages having same From Address
Messages having same Size
Messages having same Subject
Messages having same Attachment
Messages having same Attachment Extension
Messages having Viruses
Messages having same Viruses
Select Alert Type
INFORMATION
Select Action Type
No Action
Choose Quarantine Type
Anti Spam
Action Data
Rule Name
Submit
Reset

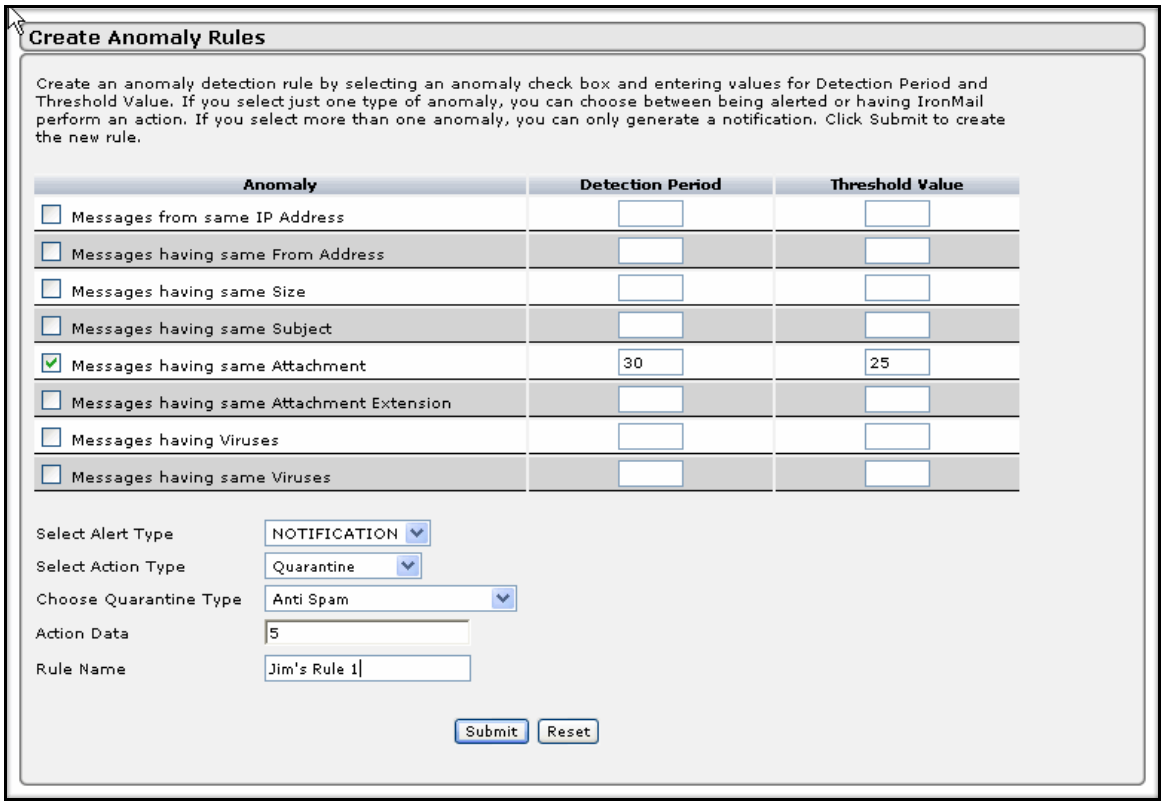
Create an anomaly detection query by selecting a type of email event's check box and entering values for Detection Period and Threshold Value. Note that if more than one email event is selected, IronMail can only generate an alert—actions are not allowed when an ADE *rule* is based on multiple events.

Anomaly Characteristic	Description	Possible ADE Response
From same IP address	If a user-defined number of messages originate from the same IP address.	Notification or Create Rule
Having same From Address	If a user-defined number of messages originate from the same email address.	Notification or Create Rule
Same size	If a user-defined number of messages are the identical size.	Notification only
Same Subject	If a user-defined number of messages have the identical subject line.	Notification or Create Rule
Same Attachments	If a user-defined number of messages have the identical attachment.	Notification or Create Rule

Same Attachment Extensions	If a user-defined number of messages have the identical file attachment extension.	Notification or Create Rule
Having virus	If a user-defined number of messages are infected with any viruses.	Notification only
Having same virus	If a user-defined number of messages are infected with the same viruses.	Notification only
Detection Period	Enter in the **Detection Period** input field a number (from 1 to 9999) representing how often, in minutes, the ADE should "wake up" to review all email that IronMail processed while it "slept." For example, if the detection period is 60 minutes, ADE will wake up and examine all messages received during each previous hour. If it finds the specified number of occurrences of the selected event-type, it will send an alert or create a rule when further messages of that type enter the *network*.	
Threshold Value	Enter in the **Threshold Value** input field a number (from 1 to 9999) representing a "threshold" or minimum number of email-types that must be detected in order for an alert to be generated or an action to be taken when additional instances occur. For example, if the threshold is 100, IronMail will wake up and examine all messages received during each previous sleep-cycle. If it finds at least 100 instances of the selected event-type, it will send an alert notifying the administrator that the "anomaly" threshold has occurred or create a rule so that when *future* instances of the anomaly occur, IronMail will perform an action on them.	
Select Alert Type	From the drop-down list, select the type of alert IronMail should issue if a specific anomaly rule is triggered. Options are shown below: 	

Select Action Type	From the drop-down list, select the action IronMail should take if a particular anomaly rule is triggered. The available "action" is contingent on the message characteristic upon which the rule is based. Not all message characteristics allow all four options. Options are:  **Note:** For message characteristics that do not support "actions," and when more than one message characteristic is specified in a query, the **Select Action Type** pick list disappears.
Choose Quarantine Type	From the drop-down list, select the quarantine type to be applied if a "Quarantine" action is configured.
Action Data	Enter any related data required by the action chosen (such as the text to be used with "Change Subject" or the time a message should be kept in quarantine).
Rule Name	Enter a name for the new rule.

The Anomaly Detection Engine can only create an "action rule" if the query is based on one message characteristic. For queries that look for more than one message characteristic, IronMail only generates alert notifications.

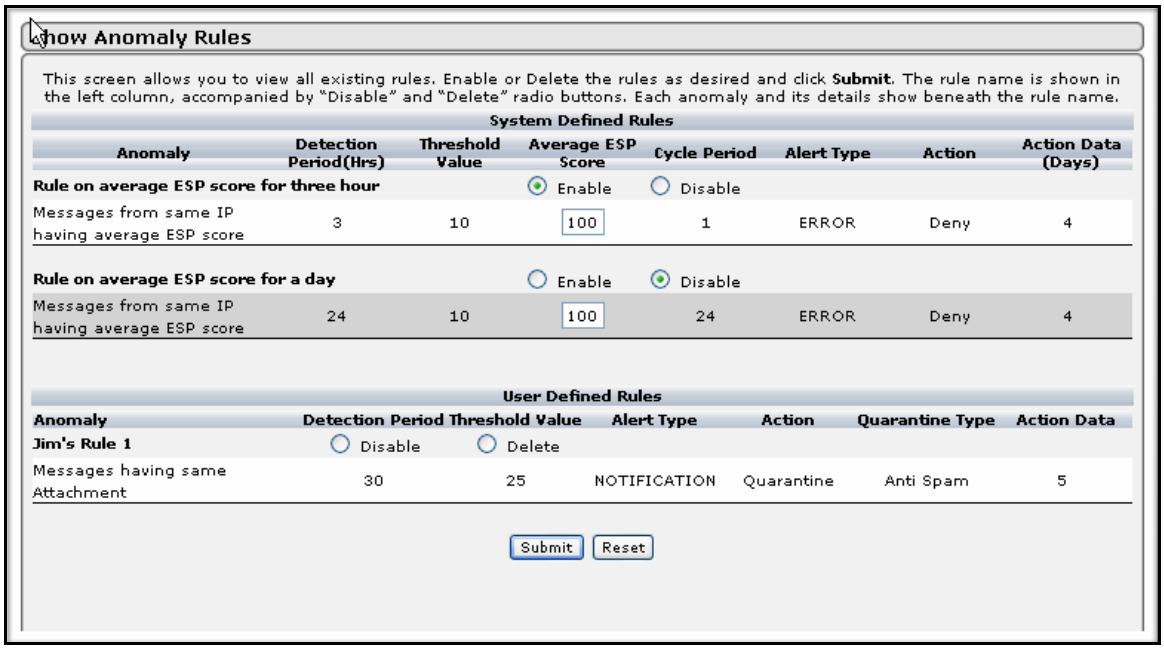

Create Anomaly Rules
Create an anomaly detection rule by selecting an anomaly check box and entering values for Detection Period and Threshold Value. If you select just one type of anomaly, you can choose between being alerted or having IronMail perform an action. If you select more than one anomaly, you can only generate a notification. Click Submit to create the new rule.
Anomaly
Detection Period
Threshold Value
Messages from same IP Address
Messages having same From Address
Messages having same Size
Messages having same Subject
Messages having same Attachment
30
25
Messages having same Attachment Extension
Messages having Viruses
Messages having same Viruses
Select Alert Type
NOTIFICATION
Select Action Type
Quarantine
Choose Quarantine Type
Anti Spam
Action Data
5
Rule Name
Jim's Rule 1
Submit
Reset

Administrators may create multiple rules based on the same message characteristic, but with differing thresholds and actions/notifications. For example, one rule can generate an email notification if ten viruses are received within *one hour*, and another rule can generate a pager alert if ten viruses are received within *5 minutes*.

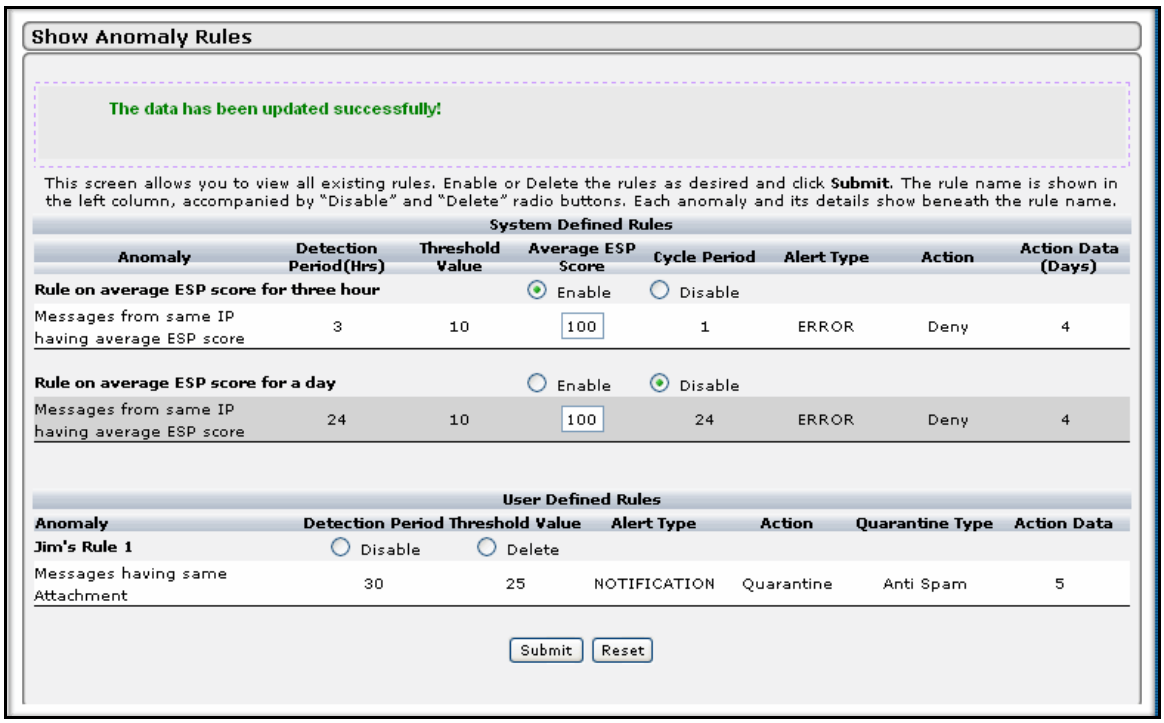
View (and edit rule values) in the Anomaly Detection Show Rules page.

Show Anomaly Rules

The Anomaly Detection Rules page displays all rules that have been created, showing their detection period, threshold, alert type, action, and action data. Edit any of the *rule* parameters as desired by entering new values.



To enable or disable a rule, click the appropriate radio button. To change the message characteristic(s) the rule is based on, delete the rule and recreate it using different message characteristics. Click **Submit** when done.



ADE Rules

Rules generated by ADE based on **IP ADDRESS** will add the offending *IP address* to the Local Deny List (*Anti-Spam > Deny Lists > Local Deny List*) Rules generated by ADE based on **FROM address** and **SUBJECT** are created in *Policy Manager* > *Mail Monitoring*. Rules generated by

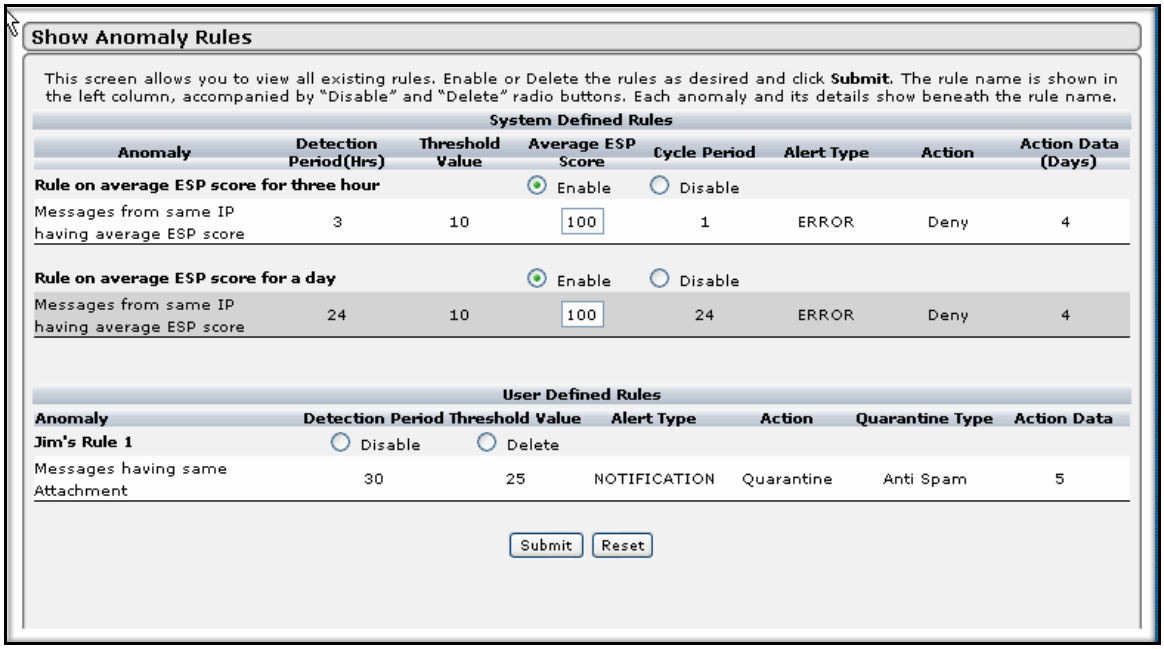
ADE based on **SAME ATTACHMENT** and **SAME ATTACHMENT EXTENSION** are created in *Policy Manager* > *Attachment Filtering*.

Connection Control

Connection Control is an IronMail feature that dramatically reduces the number of spam messages that must be processed by the appliance. It does this by reviewing the recent ESP score history of every IP address that sends messages through the IronMail appliance and then denying connections from any IP address whose history reveals they are likely to be spammers. These IP addresses are added to the Local Deny List. The number of messages that must be processed is therefore reduced because future messages from the denied IP addresses never get into the network.

Anomaly Detection Rules

The review and possible denial of connections result from two system-defined rules in IronMail's Anomaly Detection Engine. These rules are disabled by default; the Administrator must enable them (*Mail IDS > Anomaly Detection > Show Anomaly Rules).*



As indicated in the screen shot above, the rules perform two separate checks for each IP address:

- The first rule runs every hour and calculates the average ESP score for each IP address over the past three hours. If the IP address has sent 10 or more messages with an average ESP score of 100 points or higher, the IP address is denied connection to IronMail for a period of four days.
- The second rule runs every 24 hours and calculates the average ESP score for each IP address for the past 24 hours. If the IP address has sent 10 or more messages with an average ESP score of 100 points or higher, the IP address is denied connection to IronMail for a period of four days.

The rules are defined to eliminate false positives by requiring that the IP address has sent enough messages and that these messages have a high enough average ESP score to warrant denial. If the total count of all messages is high enough, but the ESP average is NOT high enough, the IP address will not be denied. Correspondingly, if the ESP average is high, but the messages count is low, the IP address will not be denied.

Should a false positive ever occur, it can be corrected through the Local Deny List.

Configuration Options

The detection periods, threshold values, cycle periods, alert types and actions for the two rules are not configurable. The only Administrator-configurable options are:

- To enable or disable each of the two rules, and
- To change the minimum average ESP score required to qualify for Connection Control.

Changes to the default configuration may be made by IronMail's Threat Response Updates (TRUs).

Special Requirements

In order for Connection Control to work, the following conditions MUST be met:

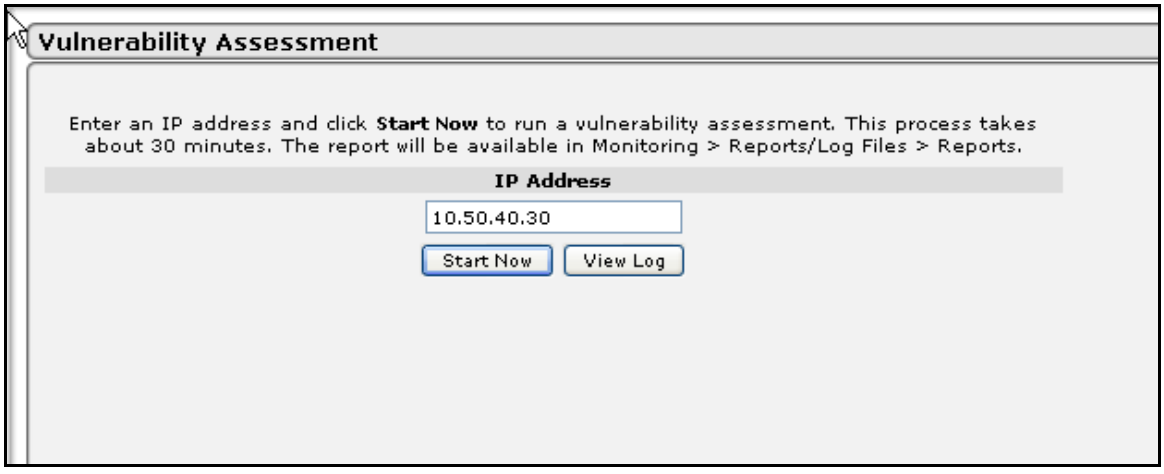
- Enterprise Spam Profiler (ESP) must be enabled;
- The IronMail utilizing the Connection Control must be the first hop into the network; and,
- Any host (such as a secondary MX) forwarding mail to the IronMail appliance, but that should not be subjected to Connection Control analysis must be added to the Allow Relay list for the IronMail.

Cleanup Cycle

When the denial period expires for a denied IP address, the cleanup cycle will remove that IP address from the Local Deny List, and connections fom that IP address will be accepted again. However, the IP address will be denied again if the IP address fails any subsequent Connection Control checks.

Vulnerability Assessment

IronMail allows administrators to scan their internal mail servers and test for any vulnerability that may be present. Specifically, it will detect every open port on the server, and identify in its subsequent report any known vulnerabilities associated with those ports. When finished, it will print its findings to a log file, viewable in IronMail's *Monitoring > Reports/Log Files > Reports > "Vulnerability Assessment."*


Vulnerability Assessment
Enter an IP address and click Start Now to run a vulnerability assessment. This process takes about 30 minutes. The report will be available in Monitoring > Reports/Log Files > Reports.
IP Address
10.50.40.30
Start Now
View Log

Enter the *IP address* of the mail server to be tested and click **Start Now**. Go grab a cup of coffee and relax for a while. The test will take approximately 30 minutes to complete.

The progress of the assessment is recorded in a log, which displays when one clicks the **View Log** button. An example appears below.

```
Thu Oct 14 11:59:39 EDT 2004:Vulnerability Assessment: requested for 10.50.40.30
Thu Oct 14 11:59:47 EDT 2004:Vulnerability Assessment: server started
Thu Oct 14 11:59:47 EDT 2004:Vulnerability Assessment beginning...
Thu Oct 14 12:04:07 EDT 2004:Vulnerability Assessment: testing ended.
Thu Oct 14 12:04:07 EDT 2004:Vulnerability Assessment: testing processes ended.
Thu Oct 14 12:04:07 EDT 2004:Vulnerability Assessment: Report is ready: VulnerabilityAssessment-
10.50.40.30-115910142004.rpt
Thu Oct 14 12:04:07 EDT 2004:Vulnerability Assessment: 10.50.40.30 all processes ended.
```

Be aware that running this test may temporarily affect the performance of the machine IronMail is scanning. The Vulnerability Assessment tool will make numerous connections to it over the course of its examination.

The results of the test are available on the Reports screen, may lead the administrator to close ports that are not needed for mail services. Specific information and recommendations may be provided for each vulnerability that is discovered.

BROWSER-BASED MAIL

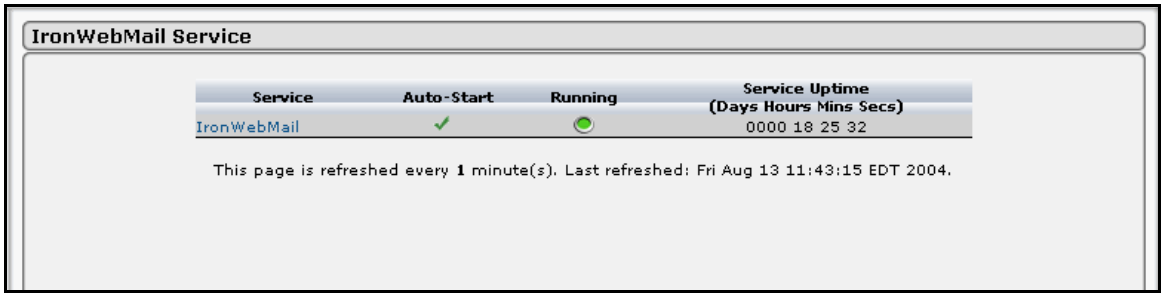
Secure WebMail

Because browser-based email continues to grow in popularity and enterprises increasingly turn to applications such as Lotus iNotes, Outlook Web Access, and GroupWise WebAccess, IronMail provides IronWebMail to offer the same protection against HTTP *network* attacks as it does for SMTP attacks. In addition to providing a "hardened face" to the web-enabled mail servers running the web mail applications, IronWebMail also offers additional security measures such as HTTPS (*SSL*) messaging, Secure Logoff, optional Strong Client Authentication, and more.

Within the IronWebMail program area, Configure HTTP Proxy, HTTP Routing, Signature Configuration, and Strong Client Authentication hyperlinks on the left side of the browser window offer navigation to pages where IronWebMail may be configured.

HTTP Proxy

Configure Secure WebMail

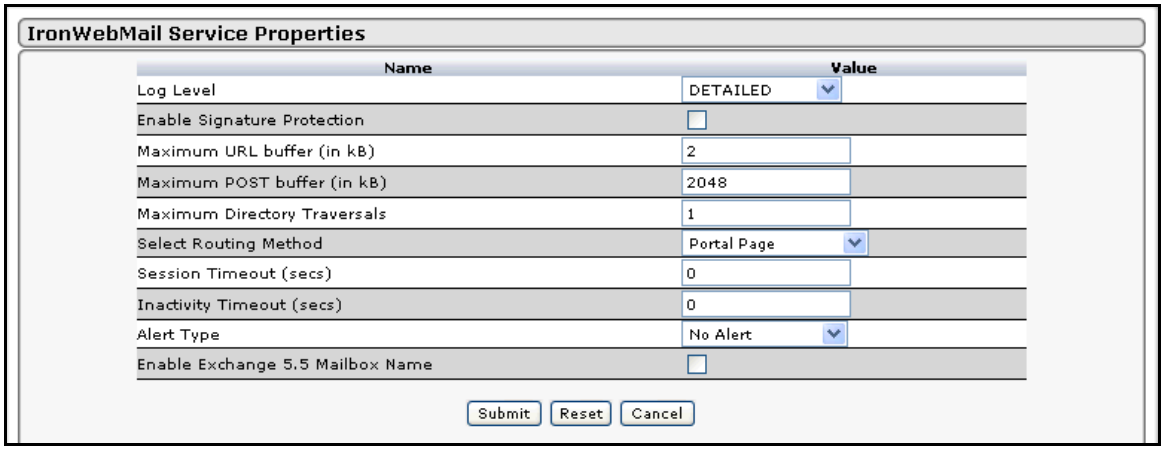


IronWebMail is an IronMail "service" or subsystem responsible for proxying HTTP/HTTPS email for a web-enabled mail system. The Configure IronWebMail Proxy page allows basic configuration of the service. The service may be started, stopped, and set to auto-start. The Configure IronWebMail Proxy table offers the following:

Field	Description
Service	The name "IronWebMail" is displayed in this column, identifying the IronMail service responsible for proxying web mail. The name is also a hyperlink that opens a secondary browser window in which various configuration options for this service may be set.
Auto-Start	The green and red "check" or "x" icons are hyperlinks. Clicking the icon hyperlink toggles the service on and off. If the icon is green, the service will begin running when IronMail restarts. If an icon is red, the service will not start on reboot. (Note that a service can continue to run after its auto-start setting is turned off. However, a stopped service cannot start running until its auto-start setting is turned on.) Unlike other services that have an auto-start option (e.g., SMTPI Service, *POP3* Service, etc.), IronMail's Health Monitor will not restart the IronWebMail Service (if it is found to be stopped for any reason) when it performs its tests on all appliance subsystems. If stopped, IronWebMail must be manually started again by clicking the red running icon (changing it back to green).

Running	This column identifies whether the service is currently running. A green light icon indicates that the service is currently running. Click the green light icon to immediately stop the service. (The green light icon turns red.) A red light icon indicates that the service is not currently running. When the IronWebMail Service is stopped, IronMail will cease proxying HTTP mail for domains it hosts.
Service Uptime	This column indicates how long the service has been running since it was last restarted. Note that the length of time (days, hours, and minutes) is static. The total uptime is refreshed each time the Configure HTTP Proxy hyperlink in the left navigation frame is clicked.

Clicking the **IronWebMail** hyperlink in the Configure IronWebMail Proxy table opens a secondary browser window in which the following IronWebMail options may be configured.



Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the amount of detail written to the log.
Enable Signature Protection	IronWebMail incorporates an Intrusion/Detection engine that examines packets of email data as it flows through the IronMail appliance. It compares *packet* information against a database of hundreds of known "attack signatures." (If a Mail IDS license was installed on IronMail, IDS signatures may be updated from the IDS Update license on a regular basis.) "Signatures" may be viewed, enabled or disabled at *IronWebMail > Signature Configuration*. Note that a handful of signatures have been disabled by default (e.g., "1568 WEB-MISC /exchange/root.asp access") because of a potential conflict with IronWebMail functionality or functionality common to some applications. Before enabling Signature Protection, ensure that someone knowledgeable with attack signatures carefully reviews the entire list of available signatures.
Maximum URL Buffer (in KB)	Buffer overflows are a common tactic for taking control of an application, such as web-enabled mail server software. By flooding the web-enabled mail server with long command strings, an attacker can trick it into running his own malicious code. Specify in this field the maximum number of bytes of data in a URL that IronWebMail will allow. (One byte roughly equates to one character of ASCII text—a 1 KB limit, therefore, allows 1,024 characters in the URL.)

Maximum POST Buffer (in KB)	To prevent hackers from using a web form's Submit action as a vehicle for attacking an internal web-enabled mail server, enter a maximum number of bytes of data allowed to be submitted in a POST method. The number should be close to the largest form action taken on the web client and submitted to the web-enabled mail server. Since large maximum limits may offer hackers the opportunity to craft dangerous "payloads," many administrators choose to limit the POST buffer size to 5-10KB, essentially disallowing the transmission of file attachments. Note that this limit applies when any action in the web mail client points to a URL. (e.g., clicking a hyperlink to compose or delete a message, or when sending a message). Note that if file attachments to web mail are allowed, the maximum POST buffer limit must be relatively high (e.g., >1,000 KB). On the other hand, large maximum limits offer hackers plenty of room to craft dangerous "payload" should they gain access to an HTTP session.
Maximum Directory Traversals	A common attack against web-enabled mail servers is to "traverse directories" using "../" in URLs (e.g., GET://http://yourdomain.com/exchange/../../../restrictedfile.cfg"). "Dot-dot-forward slash" allows navigation upward to parent directories. Either knowledge of the web-enabled mail server application in use, or dumb luck, allows hackers to traverse to files or directories on the machine running the web-enabled mail server applications. Enter a number representing the maximum number of directory traversals IronWebMail will allow. If IronWebMail detects more than this number of traversals (that is, instances of "../") in a path statement, it will automatically drop the session. And under no circumstance will IronWebMail allow a user to traverse above the directory specified in the *IronWebMail* > *HTTP Routing* tables.
Select Routing Method	IronWebMail offers a variety of routing options as it proxies email for web mail systems. Select from the pick list a routing option depending on the web mail configuration for the *network* IronWebMail is proxying. • **Path-Based Routing:** Use Path-based Routing when all internal web-enabled mail servers use a unique path string pointing to their web mail application (e.g., /exchange, /, /mail, etc.). • **Host-Based Routing:** Use Host-Based Routing when there are multiple internal web-enabled mail servers and the path strings pointing to the web mail application are identical (e.g. /). • **Portal Page:** Use the Portal Page when IronWebMail is proxying web mail specifically for one or more Outlook Web Access servers, and "True Logoff" or "Secure Logoff" is required. **Note:** the routing method selected must match the information configured under the HTTP Routing link.
Session Timeout (secs)	To close the "window of vulnerability" inherent in lengthy open sessions, IronWebMail can automatically log out users after a specified period of time. Enter a number, from 0 to 1,800, representing the number of seconds a session may remain open before IronWebMail closes it. (Users must manually log back on after IronWebMail has closed a session.) 1,800 seconds equals 30 minutes. A "0" value represents "unlimited"—IronWebMail will not close the session until a user manually logs out or closes the browser.

Inactivity Timeout (secs)	Again, to close the "window of vulnerability," IronWebMail can close a session after a specified period of inactivity. Enter a number, from 0 to 1,800, representing the number of seconds of user inactivity before IronWebMail closes the session. (Users must manually log back on after IronWebMail has closed a session.) 1,800 seconds equals 30 minutes. A "0" value represents "unlimited"—IronWebMail will not close the session until a user manually logs out or closes the browser.
Alert Type	IronMail can generate an alert (delivered by its Alert Manager) if it detects a signature-based web attack or a session or inactivity timeout. Select from the **Alert Type** pick list the level of alert IronMail's Alert Manager should generate when any of these events occur. The Alert Manager must be configured to deliver alerts for the specified level of alert and for the "class" of IronMail subsystems in which the IronWebMail subsystem currently belongs.
Enable Exchange 5.5 Mailbox Name	(This option only applies to the Portal Page configuration of IronWebMail.) Enable this option if your Exchange 5.5 software is configured to require a Mailbox Name in addition to Account Name and Password. IronMail prompts users to enter their Mailbox Name (e.g. E-Mail address) when they logon to Outlook Web Access.

HTTP Routing

IronWebMail can proxy the web sessions for users who ordinarily would have connected directly to the internal web-enabled mail servers. By sitting between users out in the Internet and the internal web-enabled mail servers, IronWebMail can protect against *network* attacks, provide *SSL* encryption of the web mail, and securely close browser sessions it proxies.

Administrators must map a "route" to the web-enabled mail server so IronWebMail knows how to proxy end users' web mail requests to the internal server hosting their mail box. The HTTP Routing hyperlink in the left navigation frame expands to offer Path-Based Routing, Host-Based Routing, and Portal Page sub-menus. Each page represents a proxy "solution" for a particular type of web mail server environment. Depending on the configuration of the internal mail server(s), one of the routing options here will be used.

Use Path-based Routing when all internal web-enabled mail servers use a *unique path string* pointing to their web mail application (e.g., /exchange, /, /mail, etc.). End users will point their browsers to IronMail's fully qualified *host name*, followed by the path string to the web mail application. IronWebMail will resolve each server's unique path string to its URL.

Use Host-based Routing when there are multiple internal web-enabled mail servers and the *path strings pointing to the web mail application are identical* (e.g. "/" or "/exchange"). Create one virtual host name/*IP address* on the DNS server for each web-enabled mail server IronWebMail proxies. The A and PTR records for each virtual host name point to IronMail. IronWebMail maps each of its virtual IP addresses to a specific internal web-enabled mail server, thus routing end users to the web-enabled mail server hosting their mail box.

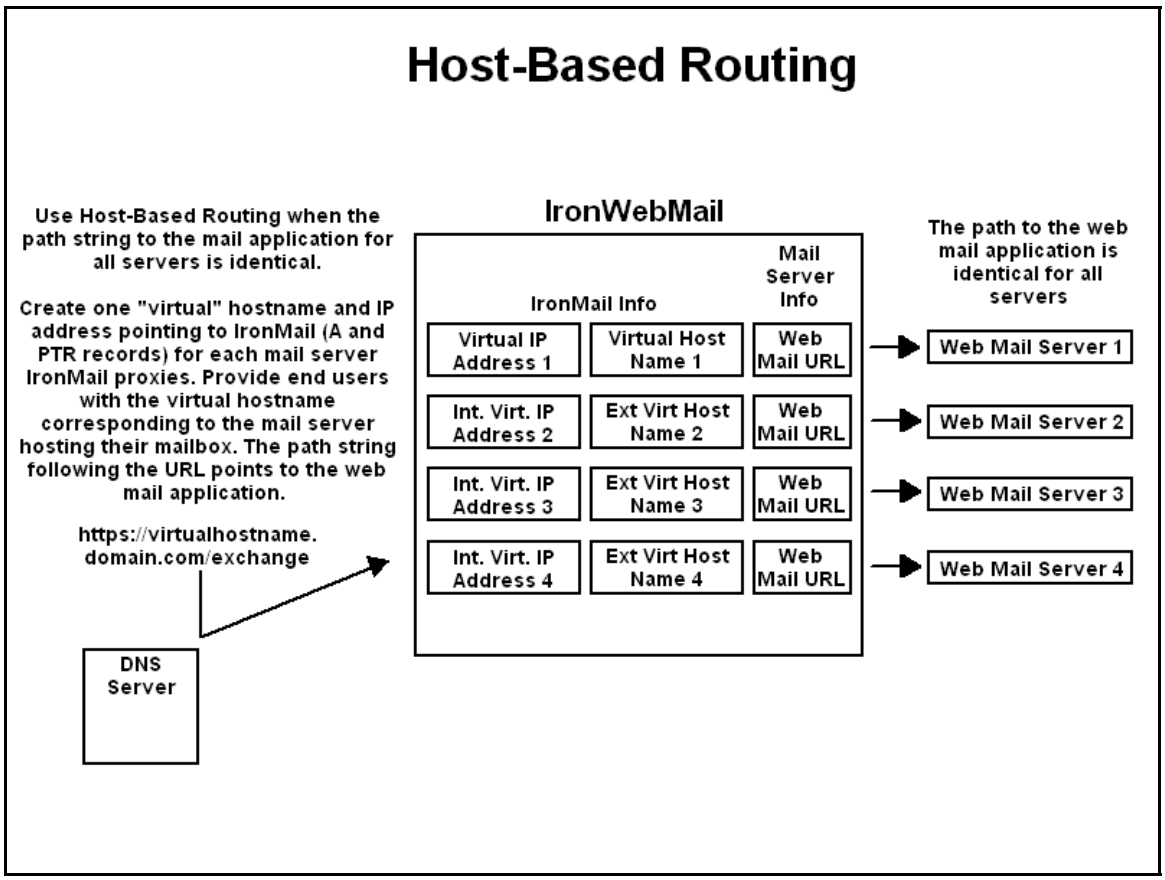
Use the Portal Page when IronWebMail is proxying web mail specifically for *one or more Outlook Web Access/Exchange servers*, and "True Logoff" or "Secure Logoff" is required. (With "True Logoff" or "Secure Logoff," IronWebMail will totally close, on logoff, the session to the web-enabled mail server so that subsequent individuals using the same open browser cannot "back in" to a web mail session.)

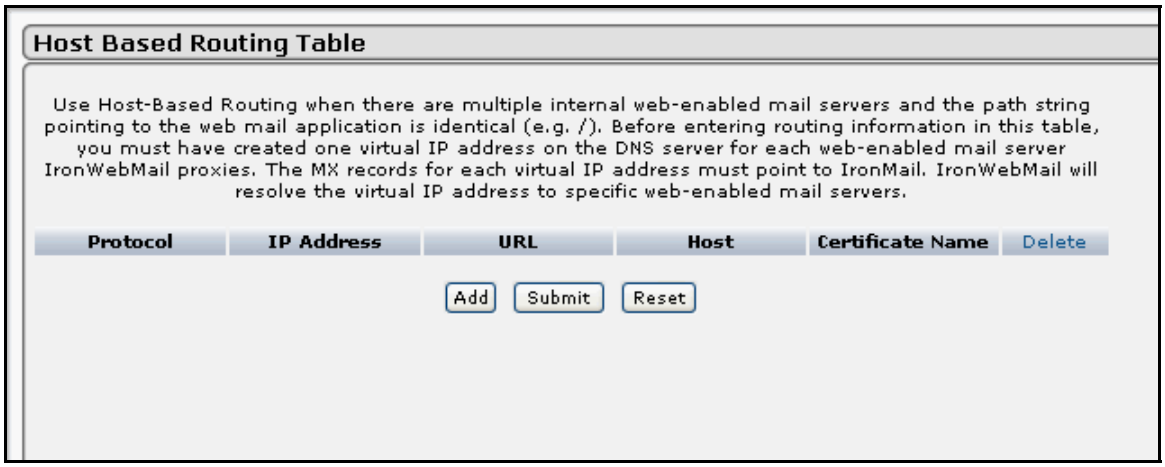
Routing recommendations for specific email environments appear in the table below.

Environment	Recommendation
Outlook Web Access	Portal Page Routing
Microsoft Exchange 5.5 and 2000	Portal Page Routing
iNotes with one server	Path-Based Routing
iNotes with multiple servers	Host-Based Routing
Groupwise with one server	Path-Based Routing
Groupwise with multiple servers	Host-Based Routing

Host-Based Routing

When there are multiple internal web-enabled mail servers using identical "path strings" to the various web mail applications, Host-based Routing provides a solution by way of "virtual IP addresses and host names." Administrators must create one virtual *IP address*/*host name* on the *DNS server* that points to IronMail (via A and PTR records) for each web-enabled mail server IronWebMail proxies. These A and PTR records point to IronMail, not the mail servers! IronWebMail maps each of the virtual IP addresses to an internal web mail server in the Host-based Routing table. End users will point their browsers to the IronWebMail virtual host name associated in the Host-Based routing table with the particular web-enabled mail server hosting their mail account.

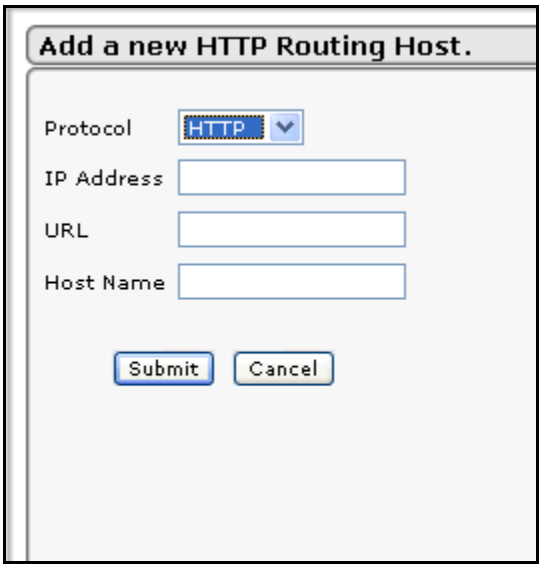

Host-Based Routing
Use Host-Based Routing when the path string to the mail application for all servers is identical.
Create one "virtual" hostname and IP address pointing to IronMail (A and PTR records) for each mail server IronMail proxies. Provide end users with the virtual hostname corresponding to the mail server hosting their mailbox. The path string following the URL points to the web mail application.
https://virtualhostname.domain.com/exchange
DNS Server
IronWebMail
IronMail Info
Mail Server Info
Virtual IP Address 1
Virtual Host Name 1
Web Mail URL
Int. Virt. IP Address 2
Ext Virt Host Name 2
Web Mail URL
Int. Virt. IP Address 3
Ext Virt Host Name 3
Web Mail URL
Int. Virt. IP Address 4
Ext Virt Host Name 4
Web Mail URL
The path to the web mail application is identical for all servers
Web Mail Server 1
Web Mail Server 2
Web Mail Server 3
Web Mail Server 4


Host Based Routing Table
Use Host-Based Routing when there are multiple internal web-enabled mail servers and the path string pointing to the web mail application is identical (e.g. /). Before entering routing information in this table, you must have created one virtual IP address on the DNS server for each web-enabled mail server IronWebMail proxies. The MX records for each virtual IP address must point to IronMail. IronWebMail will resolve the virtual IP address to specific web-enabled mail servers.
Protocol
IP Address
URL
Host
Certificate Name
Delete
Add
Submit
Reset

The Host-based Routing table displays the following information:

Field	Description
Protocol	This column shows whether IronWebMail should use the secure HTTPS or non-secure HTTP protocol between end users' browsers and itself. (Once a valid Security Certificate is installed on IronMail, it is capable of encrypting all web mail **between end users and itself**. (See *System > Certificate Manager*.) End users must specify the "HTTPS" protocol in the URL when they browse for their email if IronWebMail is configured to use it.
IP Address	The column lists the virtual IP addresses (for which a DNS A and PTR record were created). Each virtual IP address entered in this table is associated with the specific web-enabled mail server named in the **URL** field immediately to the right.
URL	This column provides the qualified *domain name* for the internal web-enabled mail server. An example of a URL is: "HTTPS://yourservername.yourdomain.com/."
Host Name	Enter the virtual fully qualified host name of the IronMail appliance (e.g. virtualironmailname.domainname.com).
Certificate	This column lists the X.509 Security Certificate that IronWebMail will use to provide a secure session between end users' browsers and itself. The list displays only X.509 Security Certificates that have been installed on the IronMail appliance.
Delete	To delete a server from the Host-based Routing table, select its **Delete** check box and click **Submit**.

Clicking "Add" on the Host Based Routing Table opens a secondary browser to be used in adding a new host to the system.



Field	Description
Protocol	Select the proper protocol that IronMail should use between the end users' browsers and itself (secure HTTPS or non-secure HTTP). End users must specify the "HTTPS" protocol in the URL when they browse for their email if IronWebMail is configured to use it.
IP Address	Enter the virtual IP addresses (for which a DNS A and PTR record are created). Each virtual IP address entered in this table is associated with the specific web-enabled mail server named in the **URL** field.
URL	Enter the qualified domain name for the internal web-enabled mail server. The URL must include the "protocol prefix" (HTTP:// or HTTPS://) as this indicates whether the connection between IronMail and the internal mail server is secure or not. The URL must not include the path string to the web-enabled mail server application, but must include a trailing forward slash at the end of the URL. An example of a URL is: "HTTPS://yourservername.yourdomain.com/." **Note:** Neither Exchange 5.5 nor Exchange 2000 supports the HTTPS protocol. Additionally, host-based routing for an iNotes server requires that the external and internal protocols "match." That is, if users connecting to IronMail use HTTPS in the URL, then IronMail's connection to the Domino web server must also use HTTPS.
Host Name	Enter the virtual fully qualified host name of the IronMail appliance (e.g. virtualironmailname.domainname.com).

Provide end users with the following URLs:

https://virtualironmailname.yourdomain.com/ (for GroupWise users)

https://virtualironmailname.yourdomain.com/exchange (for Exchange users)

https://virtualironmailname.yourdomain.com/mail/username.nsf (for iNotes users) If Web Delivery Redirect from Notes.Net is being used, this may change the URL that end users are required to enter.

where

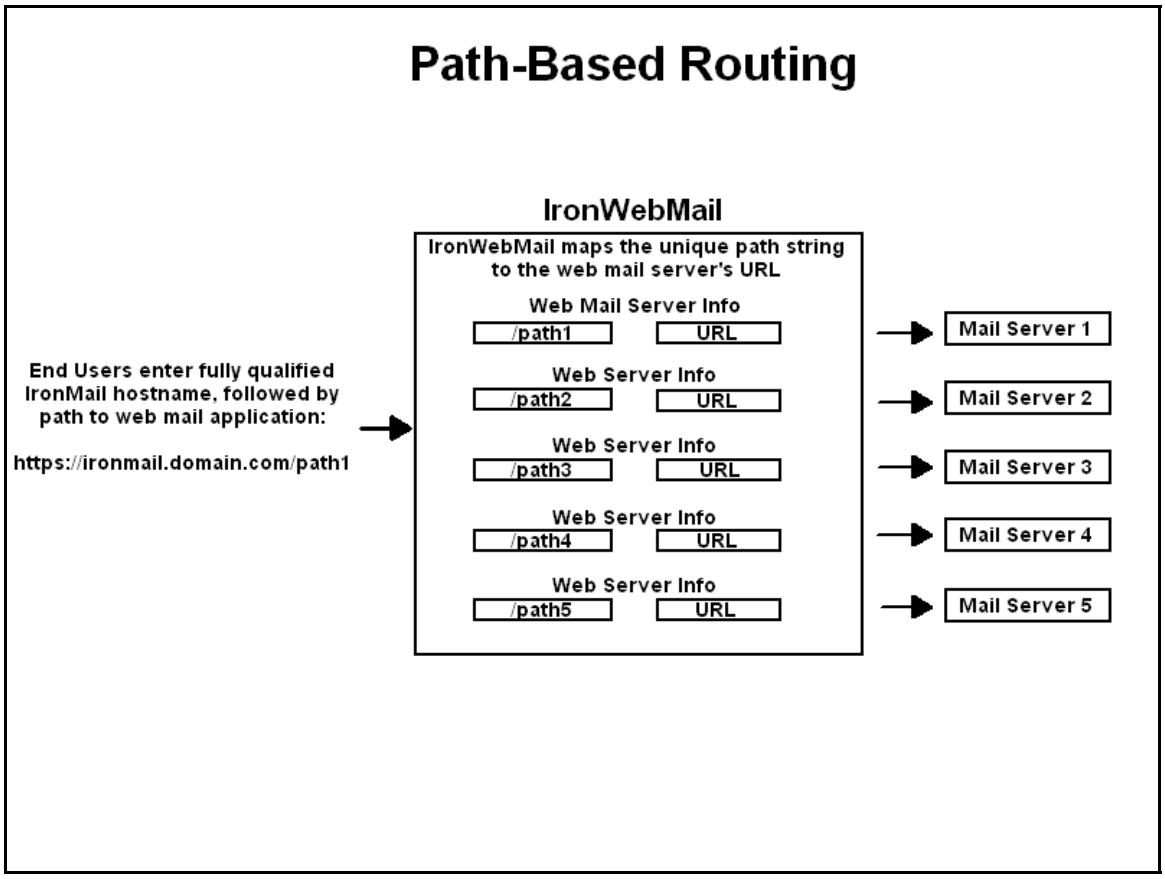
- **virtualironmailname** is the virtual IronMail host name associated with the web-enabled mail server hosting the user's mail box.

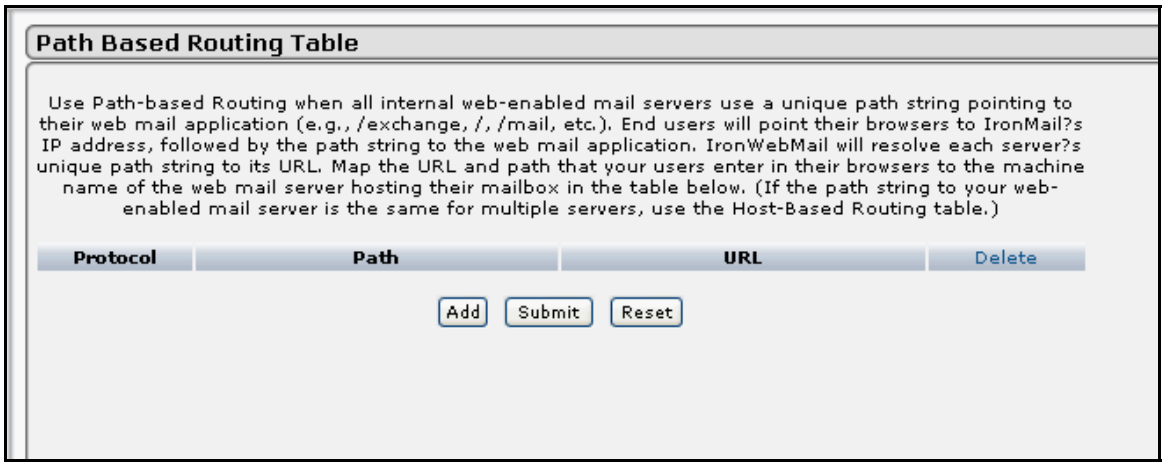
- **yourdomain.com** is the domain to which IronMail belongs.

Note that if IIS is running on the web-enabled mail server, Windows NT's Challenge Response (NTLM Directory Security in the Internet Service Manager) must be disabled. Use Basic Authentication only. See the **Microsoft knowledgebase article Q317627** for more information on NTLM Directory Security.

Path-Based Routing

Path-based Routing is used when all internal web-enabled mail servers use a unique path string pointing to their web mail application. IronWebMail maps the unique path string to the URL of each web-enabled mail server.




Path Based Routing Table
Use Path-based Routing when all internal web-enabled mail servers use a unique path string pointing to their web mail application (e.g., /exchange, /, /mail, etc.). End users will point their browsers to IronMail?s IP address, followed by the path string to the web mail application. IronWebMail will resolve each server?s unique path string to its URL. Map the URL and path that your users enter in their browsers to the machine name of the web mail server hosting their mailbox in the table below. (If the path string to your web-enabled mail server is the same for multiple servers, use the Host-Based Routing table.)
Protocol
Path
URL
Delete
Add
Submit
Reset

The Path-based Routing table shows the following information:

Field	Description
Protocol	The **Protocol** column indicates whether IronWebMail will use the secure HTTPS or non-secure HTTP protocol between end users' browsers and itself. End users must specify the "HTTPS" protocol in the URL when they browse for their mail if IronWebMail is configured to use it.
Path	This column shows the path to the web-enabled mail server application. The "path string" for each web-enabled mail server must be unique, e.g., "/exchange," "/mail," and "/" (GroupWise requires a single forward slash—"/"—as the path). If the path strings are not unique, use Host-based Routing.
URL	The column lists the fully qualified *host name* (or the *IP address*) in the **URL** input field of the web-enabled mail server that IronWebMail will proxy. Include the protocol prefix (HTTP:// or HTTPS://) specifying whether the connection between IronMail and the internal server is secure or not. The URL must also include the trailing "path string" specified in the Path input field above, and a trailing forward slash at the very end. Note that neither Exchange 5.5 nor 2000 supports the HTTPS protocol. An example of a URL is: http://exchange1.domain.com/exchange/.
Delete	Select a server's **Delete** check box and click **Submit** to delete the server from the Path-based Routing table.

Clicking "Add" on the Path Based Routing Table opens a secondary browser to be used in adding a new path to the system.

Field	Description
Protocol	Specify from the **Protocol** pick list whether IronWebMail should use the secure HTTPS or non-secure HTTP protocol between end users' browsers and itself. End users must specify the "HTTPS" protocol in the URL when they browse for their mail if IronWebMail is configured to use it.
Path	Enter the path to the web-enabled mail server application. The "path string" for each web-enabled mail server must be unique, e.g., "/exchange," "/mail," and "/" (GroupWise requires a single forward slash—"/"—as the path). If the path strings are not unique, use Host-based Routing.
URL	Enter the fully qualified host name (or the IP address) in the **URL** input field of the web-enabled mail server IronWebMail will proxy. Include the protocol prefix (HTTP:// or HTTPS://) specifying whether the connection between IronMail and the internal server is secure or not. The URL must also include the trailing "path string" specified in the Path input field above, and a trailing forward slash at the very end. **Note:** Neither Exchange 5.5 nor Exchange 2000 supports the HTTPS protocol. An example of a URL is: http://exchange1.domain.com/exchange/.
Host Name	Specify IronMail's fully qualified host name. IronWebMail will use this to resolve the machine name to its IP address.

Typical Configurations

A typical configuration for OWA 5.5 is:

- **Protocol:** HTTP
- **Path:** /exchange
- **URL:** http://owaserver.company.com/exchange
- **Exchange 2000:** Off
- **Host Name:** ironmail.company.com

A typical configuration for OWA 2000 is:

- **Protocol:** HTTP
- **Path:** /exchange

- **URL:** http://owaserver.company.com/exchange
- **Exchange 2000:** On
- **Host Name:** ironmail.company.com

Application-specific notes:

Outlook Web Access (versions 5.5 & 2000):

Unless the Exchange administrator manually edited the path to the OWA application, the default path for OWA is "/exchange." If the path was modified on the Exchange server, ensure that the same path is entered in IronWebMail's Path input field.

Outlook Web Access (version 2000 only)

Two entries in the Path-based Routing table are required for a Microsoft Exchange 2000 web-enabled mail server. One entry must contain the normal path string "/exchange." In addition to that, however, a second entry is required to point IronWebMail to images used by the OWA application. Therefore, create a second entry for the Exchange 2000 server using "/exchweb" as the image path string in the **Path** input field. (End users do not use this second string in their URL when pointing their web browsers to IronMail.)

IIS

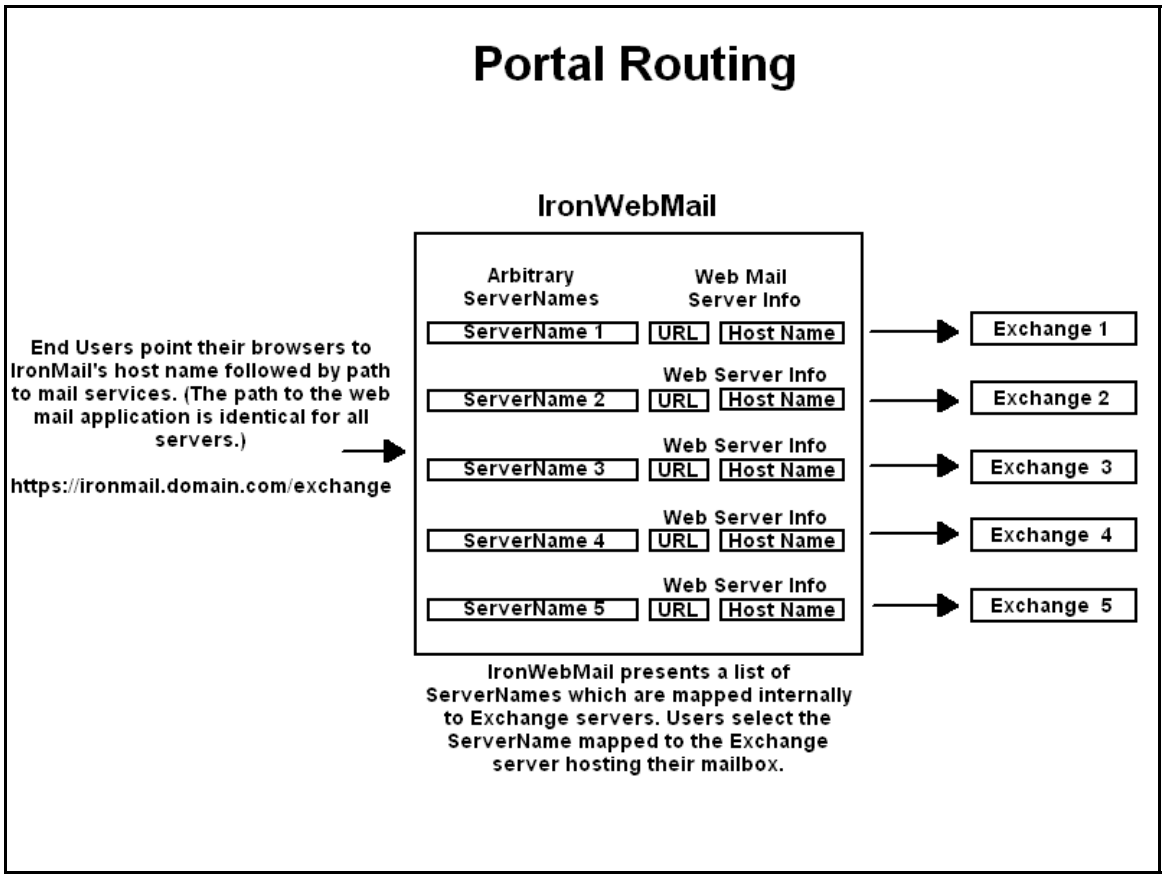
Windows NT's Challenge Response (NTLM Directory Security in the Internet Service Manager) must be turned off if IIS is employed on the web-enabled mail server. Use Basic authentication only on the IIS server.

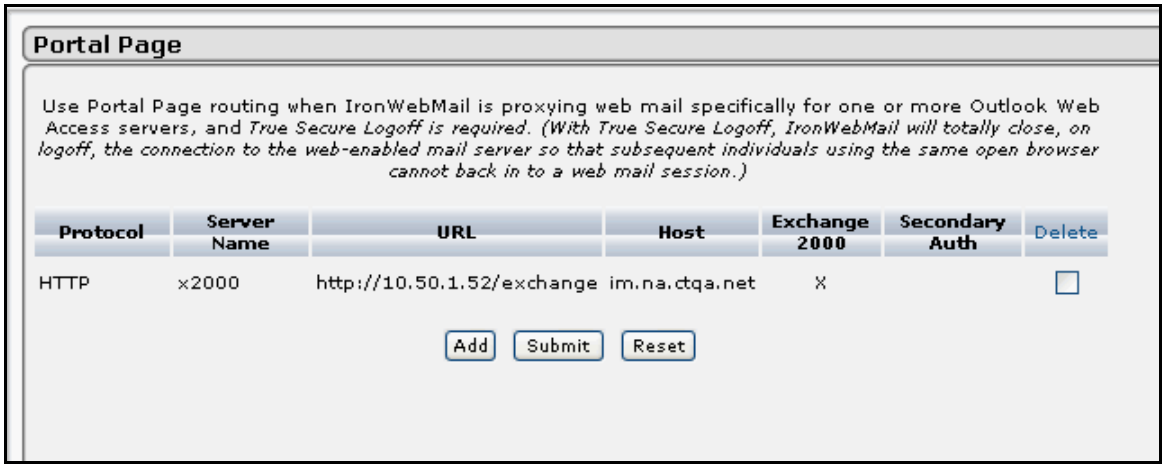
Lotus iNotes

Two entries in the Path-based Routing table are required for each Lotus iNotes web-enabled mail server. One entry must contain the normal path string "/mail." In addition to that, however, a second entry is required to point IronWebMail to images used by the iNotes application. Therefore, create a second entry for the iNotes server using "/icon" as the image path string in the **Path** input field. (End users do not use this second string in the URL when pointing their web browsers to IronMail.)

Portal Page Routing

Use the routing table in the Portal Page only if the internal web mail system employs one or more Microsoft Exchange/Outlook Web Access servers. When IronWebMail routing is configured in this Portal Page, "True/Secure Logoff" for Microsoft Exchange is automatically enabled. That is, IronWebMail will guarantee that HTTP/HTTPS sessions are closed completely when end users finish browsing for their email.



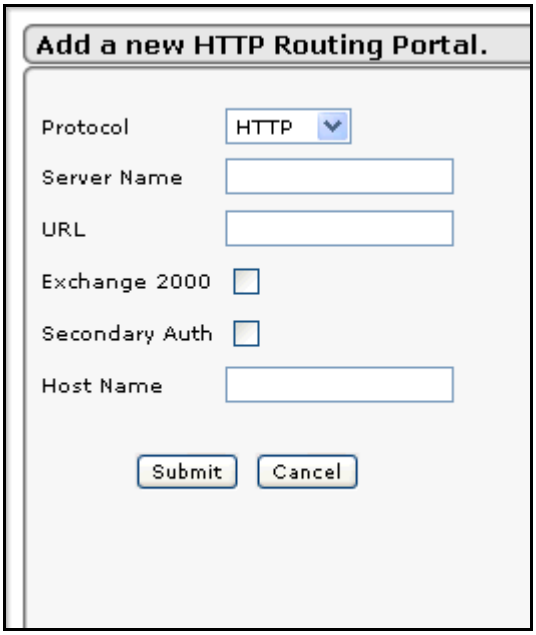

Portal Page
Use Portal Page routing when IronWebMail is proxying web mail specifically for one or more Outlook Web Access servers, and True Secure Logoff is required. (With True Secure Logoff, IronWebMail will totally close, on logoff, the connection to the web-enabled mail server so that subsequent individuals using the same open browser cannot back in to a web mail session.)
Protocol
Server Name
URL
Host
Exchange 2000
Secondary Auth
Delete
HTTP
x2000
http://10.50.1.52/exchange
im.na.ctqa.net
X
Add
Submit
Reset

The Portal Page routing table requests the following information:

Protocol	The column displays a list showing whether IronWebMail should use the secure HTTPS or non-secure HTTP protocol between end users' browsers and itself. End users must specify the "HTTPS" protocol in the URL when browsing for their email if IronWebMail is configured to use it.
Server Name	This column lists the "server names" (arbitrary names used only by IronWebMail to map to the actual mail servers configured in the URL and *Host Name* field on the "Add HTTP Routing Portal" screen).

URL	The table shows the URL (or *IP address*) of the web-enabled mail server to be associated with each Server name identified above. **Note:** Neither Exchange 5.5 nor Exchange 2000 supports the HTTPS protocol. Configuration information about Exchange is available in Appendix 3.
Host	This column shows the host name associated with each port.
Exchange 2000	Indicates by the check box if this server is running Outlook Web Access/Exchange 2000.
Secondary Auth	This check box indicates that for a particular portal secondary authorization has been configured. IronWebMail will present a single logon (with a secondary authentication area) to the end user, but pass the username and password both to the mail server as well as the authentication server. If either authentication fails, IronWebMail will drop the session.
Delete	To delete a server from the Portal Page routing table, select its **Delete** check box and click **Submit**.

Clicking "Add" on the Portal Page screen displays a secondary window that allows the Administrator to add a new portal to the system.



Field	Description
Protocol	Specify from the **Protocol** pick list whether IronWebMail should use the secure HTTPS or non-secure HTTP protocol **between end users' browsers and itself**. (Once a valid Security Certificate is installed on IronMail, it is capable of encrypting all web mail between end users and itself.) End users must specify the "HTTPS" protocol in the URL when browsing for their email if IronWebMail is configured to use it.

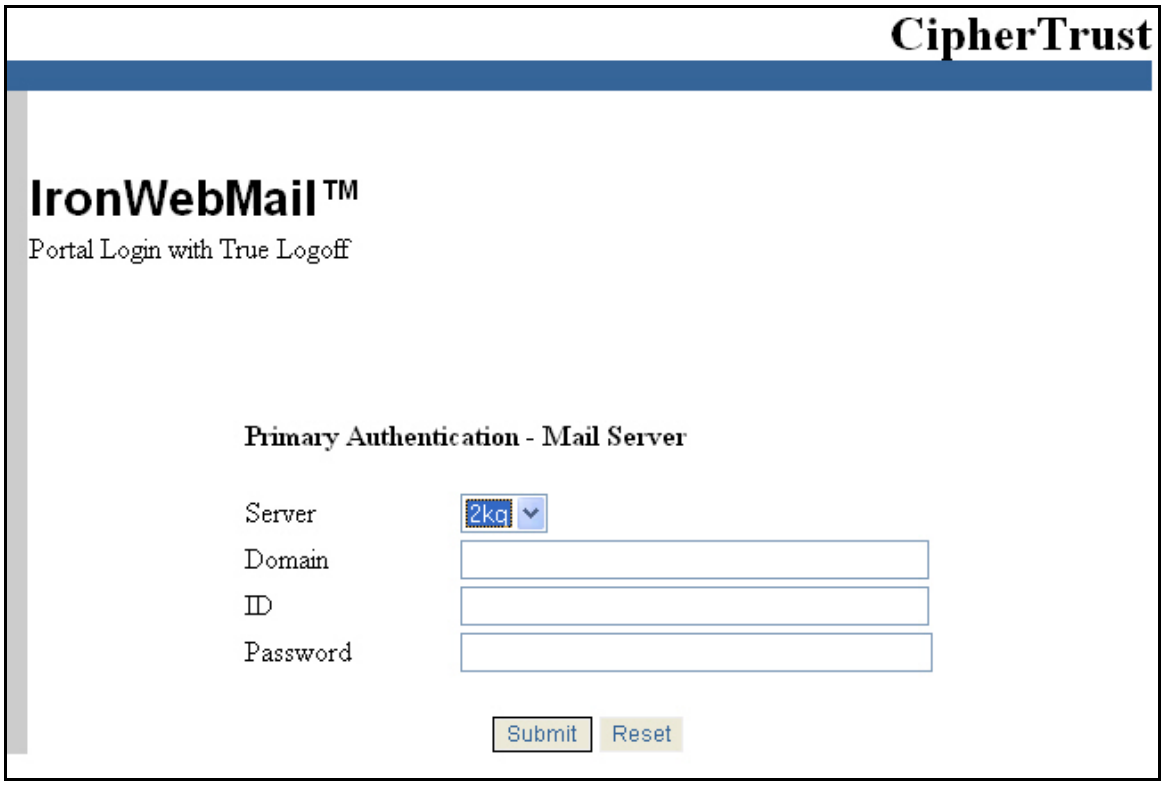
Server Name	Provide a "server" name for a web-enabled mail server. (The "server" name entered here is an arbitrary name, used only by IronWebMail to create a map to the actual web-enabled mail server specified in the **URL** and **Host Name** input fields.) When end users make their initial HTTP(s) connection, IronWebMail will present a browser window listing the "server names" for all mail servers it is hosting. Users will select the Server name associated with the mail server hosting their mail box.
URL	Enter the URL (or IP address) of the web-enabled mail server to be associated with the Server name identified above. **Note:** Neither Exchange 5.5 nor Exchange 2000 supports the HTTPS protocol.
Exchange 2000	Select the **Exchange 2000** check box only if this server is running Outlook Web Access/Exchange 2000.
Secondary Auth	If the internal web mail system uses RSA SecurID® for user authentication, select the **Secondary Auth** check box. IronWebMail will present a single logon (with a secondary authentication area) to the end user, but pass the username and password both to the mail server as well as the authentication server. (If either authentication fails, IronWebMail will drop the session.) **Note:** RSA SecurID® must already be configured and integrated into Outlook Web Access before IronWebMail can proxy web mail sessions using this authentication method. IronWebMail only supports RSA SecurID® in OWA environments.
Host Name	Enter the fully qualified host name of the web-enabled mail server (e.g. servername.domainname.com).

Note that some users' browsers may freeze when accessing the OWA web server or display a "Cannot render image" message. This is a "browser issue." The problem is resolved by clearing the browser's cache and restarting the browser.

If a user attempts to logon to the Outlook Web Access server and the session fails because of an incorrectly-typed username or password, IronWebMail records this as a "logon failure" in the IronWebMail Daily Report. IronWebMail only counts this failure when an OWA logon at IronWebMail's Portal Page fails.

IronWebMail Portal Login

The IronWebMail Portal Login page provides end users with secure browser-based access to email and internal applications. When IronWebMail routing is configured in this Portal Page, "True/Secure Logoff" for Microsoft Exchange is automatically enabled. This ensures that IronWebMail HTTP/HTTPS sessions are closed completely when end users finish browsing for their email.



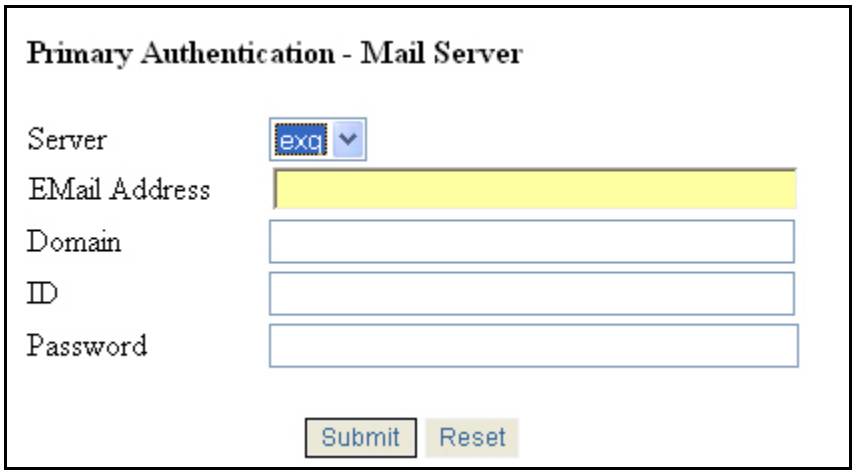
The Portal Login page offers a drop-down list with a selection of servers if multiple web-enabled mail servers.

The Portal Login page requests the following information:

Server	The user selects a "server" name for a web-enabled mail server. Users will select the Server name associated with the mail server hosting their mail box. When end users make their initial HTTP(s) connection, IronWebMail will present a drop-down list with the "server names" for all mail servers it is hosting.
Domain	Users enter the *domain name* of the web-enabled mail server.
ID	Users enter their user ID.
Password	Users enter their password.

End users click **Submit** to logon to the mail server.

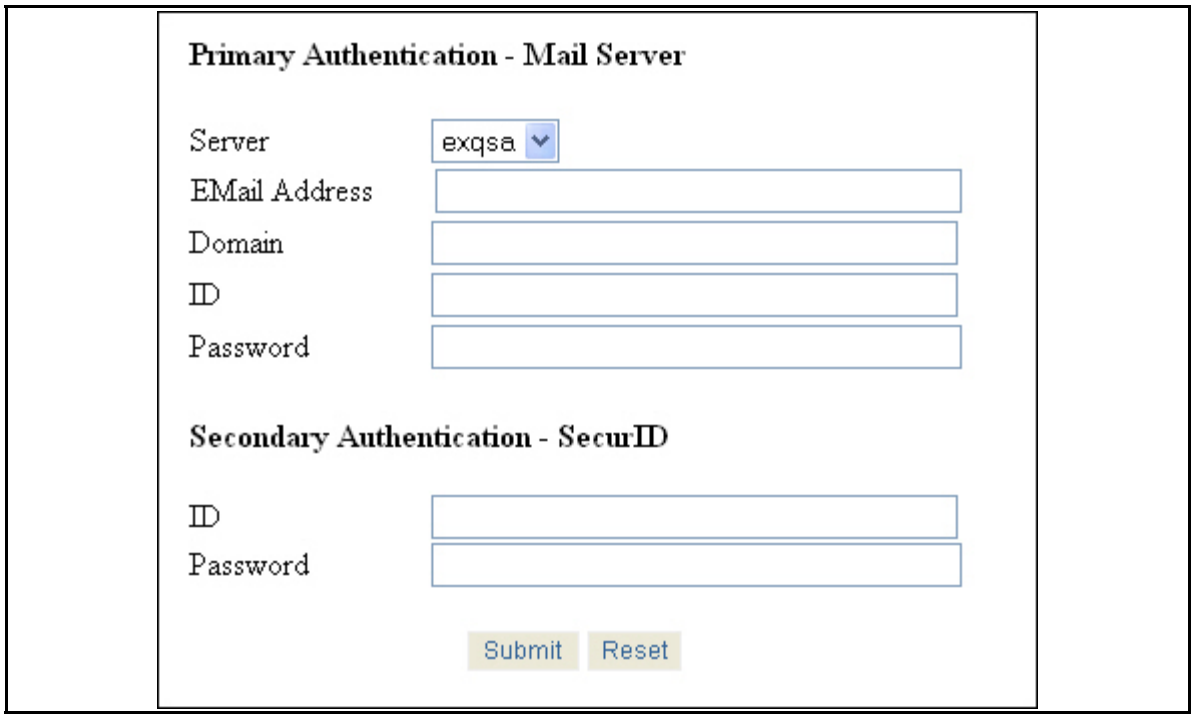
The following shows the Portal Login page Authentication area with the Email address option enabled. **Note:** the IronWebMail can be configured for installations where only selected servers have the Mailbox name option enabled. In cases where the Maibox name option is not enabled, the **EMail Address** field does not appear on the login page.



Secondary Authentication

If the internal web mail system uses RSA SecurID® for user authentication, IronWebMail will present a single logon (with a secondary authentication area) to the end user, but pass the username and password both to the mail server as well as the authentication server (If either authentication fails, IronWebMail will drop the session).

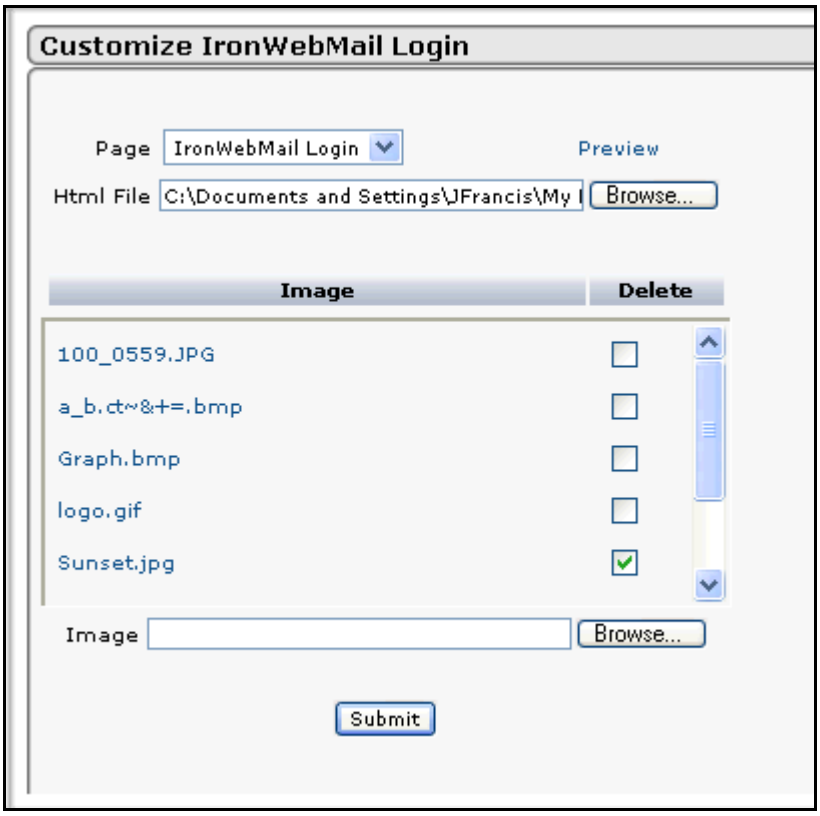
Secondary Authentication is configured on the Portal Page Routing page.



Note: RSA SecurID® must already be configured and integrated into Outlook Web Access before IronWebMail can proxy web mail sessions using this authentication method. IronWebMail only supports RSA SecurID® in OWA (Outlook Web Access) environments.

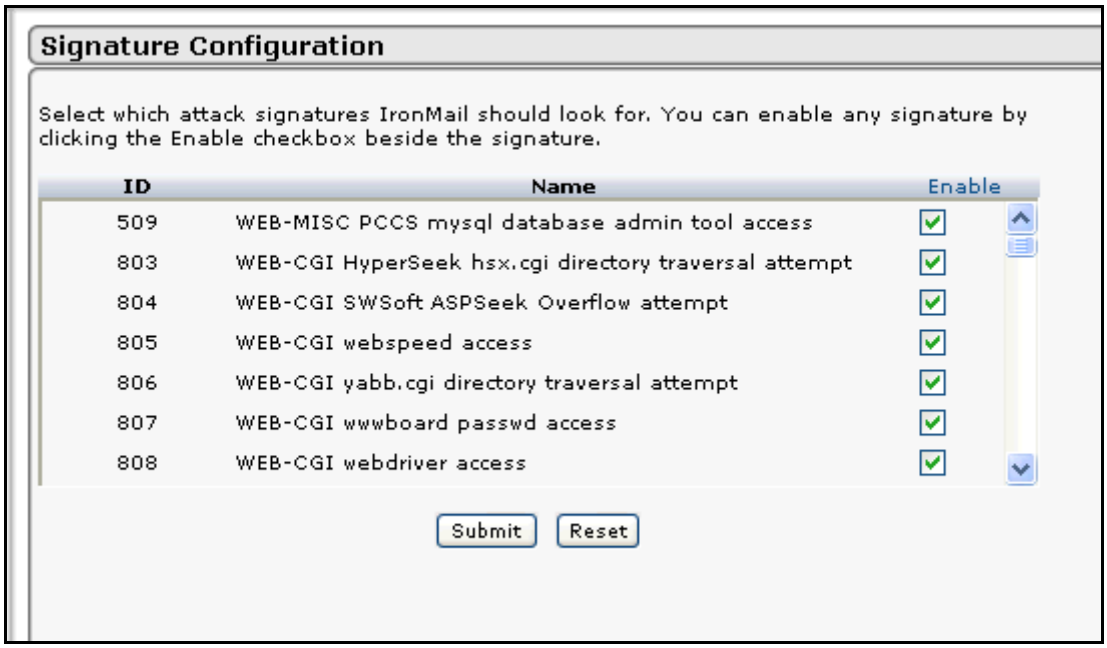
Custom IWM Page

The IronWebMail login page may be customized to promote the enterprise's company identity. More detailed information about customizing screens may be found in the Customizing Pages chapter of this manual.



Signature Configuration

IronWebMail provides real-time detection of attempted attacks through its intrusion/detection engine. By examining all packets passing across port 80 or secure port 443, it can see if they match “signatures” of known attacks. Furthermore, IronWebMail uses “protocol analysis” to overcome hackers’ URL path obfuscation techniques, like the insertion of hex, double-hex, and UNICODE strings, designed to circumvent signature detection.

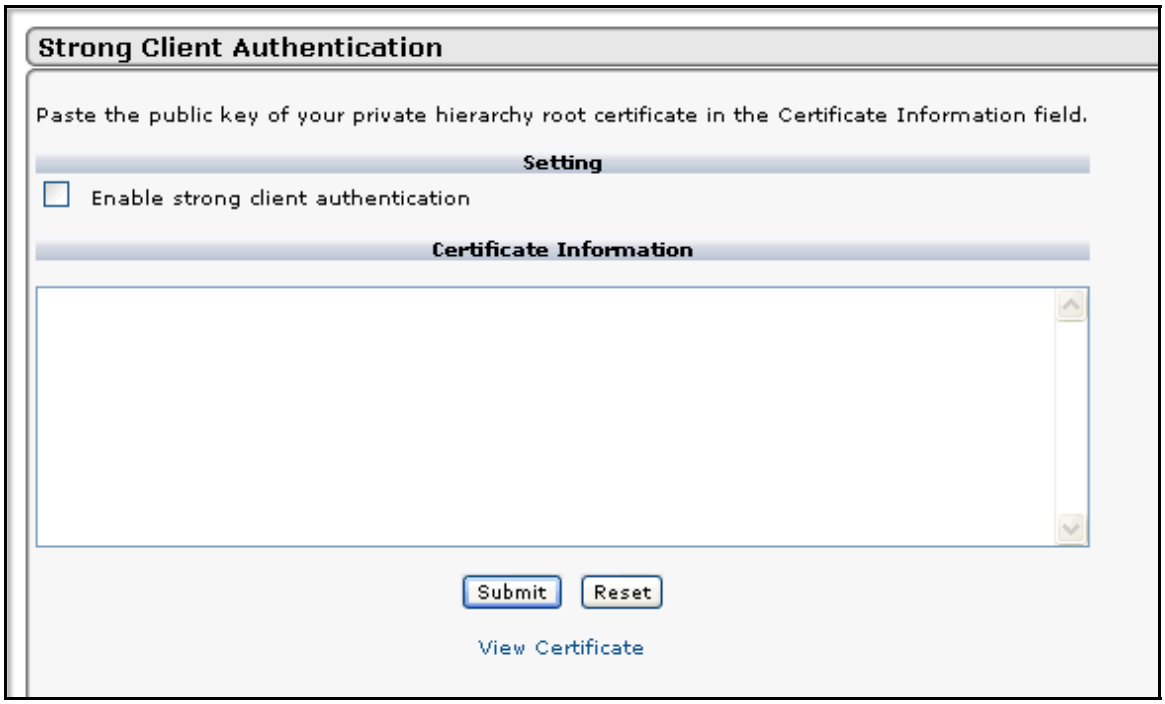

Signature Configuration
Select which attack signatures IronMail should look for. You can enable any signature by clicking the Enable checkbox beside the signature.
ID
Name
Enable
509 WEB-MISC PCCS mysql database admin tool access
803 WEB-CGI HyperSeek hsx.cgi directory traversal attempt
804 WEB-CGI SWSoft ASPSeek Overflow attempt
805 WEB-CGI webspeed access
806 WEB-CGI yabb.cgi directory traversal attempt
807 WEB-CGI wwwboard passwd access
808 WEB-CGI webdriver access
Submit
Reset

Configure which attack signatures IronWebMail should use from this window. When a signature is "checked," IronWebMail will look for that potential attack as it examines packets passing through it. (The **Enable** hyperlink at the top of the column toggles all signatures on or off.) Click **Submit** after selections have been made.

Failure to use Signature Protection negatively affects email security.

Strong Client Authentication

Just as the IronMail appliance uses a "server certificate" to authenticate itself to other servers, "client certificates" may be installed on end users' browsers so they may authenticate themselves to IronWebMail when sending and receiving their web mail. Administrators must request a Private Hierarchy Root Certificate from a Trusted Root Certificate Authority, and use that to issue client certificates to users in their *network*. The public key of the Private Hierarchy Root Certificate must be installed in IronWebMail so it can validate end users. If Strong Client Authentication is enabled, only those individuals using a browser containing a valid client certificate may send and receive email via IronWebMail's proxy service.



Select **Enable strong client authentication** to "turn on" this option. You must provide IronMail with the public key of your Private Hierarchy Root Certificate.

Each time users logon to IronWebMail's proxy service, a "Client Authentication" dialog box appears on-screen, prompting them to select the Security Certificate installed in their browser. (If they have more than one certificate installed, ensure that they select the root certificate whose corresponding public key was pasted into IronWebMail's Strong Client Authentication window.) After clicking **OK**, the user is logged onto their web-enabled mail server.

Failure to use Strong Client Authentication negatively affects email security. Strong Client Authentication is applicable for those IronWebMail routing configurations for which the *protocol* setting is HTTPS (secure) and not for HTTP (non-secure).

Installing Public Keys

Follow the instructions below to paste the public key of your private Hierarchy Root Certificate into the Certificate Information text field.

1. From any Internet Explorer browser window, pull down the **Tools** menu to "**Internet Options**."
2. Select the "**Content**" tab of the Internet Options page and click the **Certificates** button.
3. Select the "**Personal**" tab in the Certificates page. Then select the personal certificate installed in your browser and click the **View** button.
4. In the resulting Certificate page, select the "**Details**" tab and click the **Copy to file...** button. This launches a simple Wizard to export your certificate. The first step of the Wizard requires you to select an export certificate format. Select the second option, "**Base-64 encoded X.509 (.CER)**." Follow the remaining prompts to name and select a destination for the exported certificate.
5. Open the certificate file you just saved to disk in your favorite text editor. (Ensure that the application can "see all files"—the certificate file extension is ".cer.") Copy the entire contents of the certificate file and paste into IronMail's Certificate Information text field.

6. Click **Submit** to save the input.

MESSAGE SERVICES

Examining Messages

Once IronMail has determined that a connection is legitimate, it then scans each message through that connection for known and potential threats. This is a gateway security function because it does not deliver, or allow into your *network*, any message found to be harmful, whether due to viruses, sensitive or libelous content, Trojan horses, spam, pornography, etc.

IronMail scans and detects known viruses by integrating the Authentium™, Sophos™ and/or McAfee™ industry-leading anti-virus technologies. IronMail ensures timely virus detection with anti-virus file definition update-checking as often as once an hour and installed automatically. IronMail has additional tools, such as attachment filtering and content filtering, to block harmful messages, providing you many options for responding to unauthorized files or content as they attempt to enter the network.

To ensure maximum protection, particularly against new, multi-faceted threats, IronMail includes CipherTrust's patented heuristic, statistical anomaly engine. This technology allows IronMail to detect patterns of viruses, spam or other threats without requiring pre-installed signatures or keywords. The Anomaly Detection Engine is intelligent—not only does it detect, without user intervention, virus and spam attacks, but it can also automatically create rules that block all future messages from offending senders.

Messages that are allowed to enter IronMail pass through two initial queues that prepare them for inspection by IronMail features. The two queues are:

- The Rip Queue, which separates the email message into its logical parts (header information, subject, body, attachments, etc.), and
- The Content Extraction queue, which identifies formats (the types of *MIME* parts) and extracts text from the message body so it can be analyzed according to IronMail policies.

The tools that use the format information and the extracted text are:

- Attachment Filtering - to identify the format and file type of email message MIME parts
- Content Filtering - to analyze the extracted text
- Anti-Virus - for extension override
- Anti-Spam - format and text for Content Filtering in ESP and Bayesian Filtering
- ADE - for rules created on attachments
- Message Stamping - to identify the body parts that can be stamped

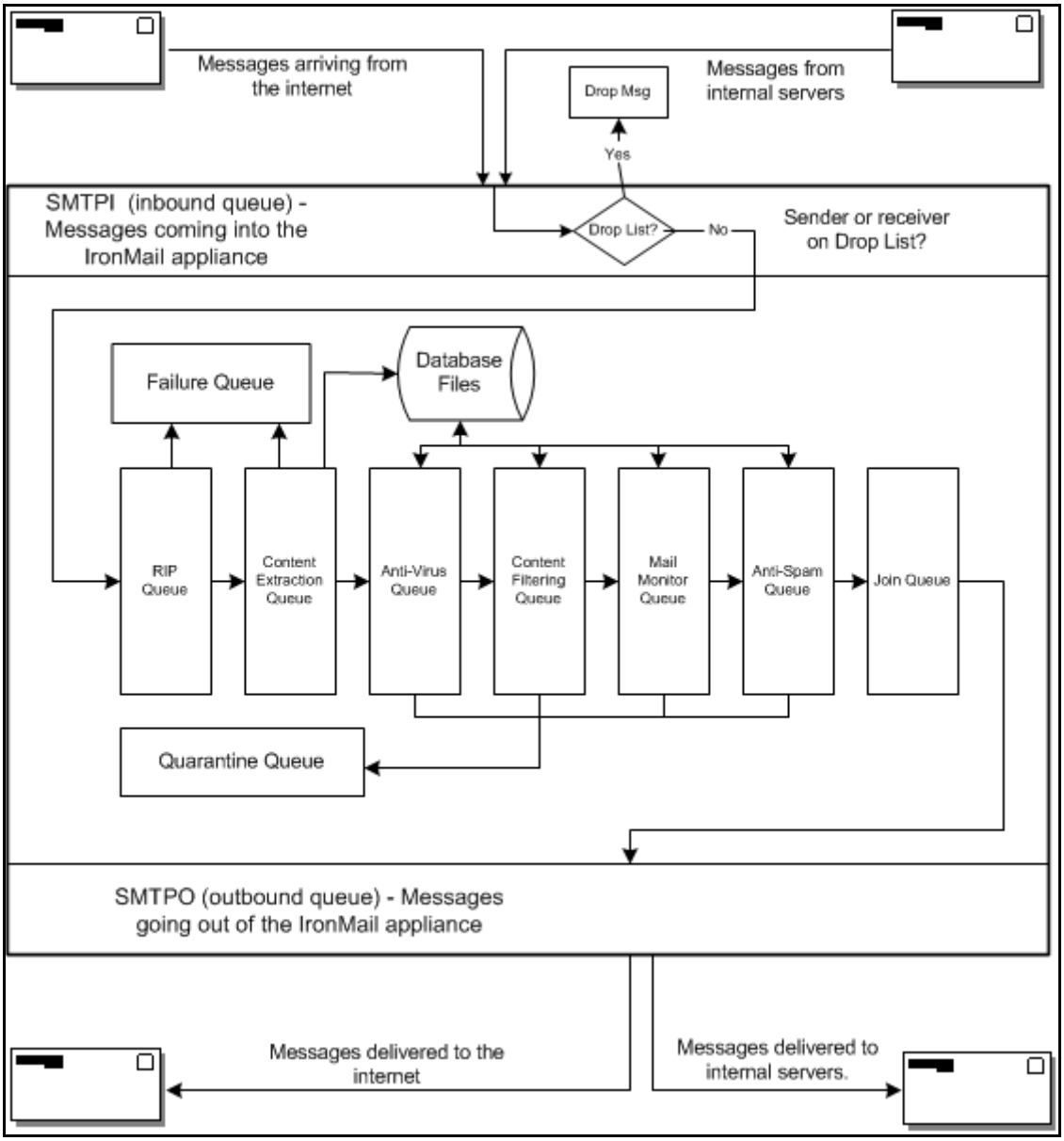
IronMail's Queues

Introducing the Queues

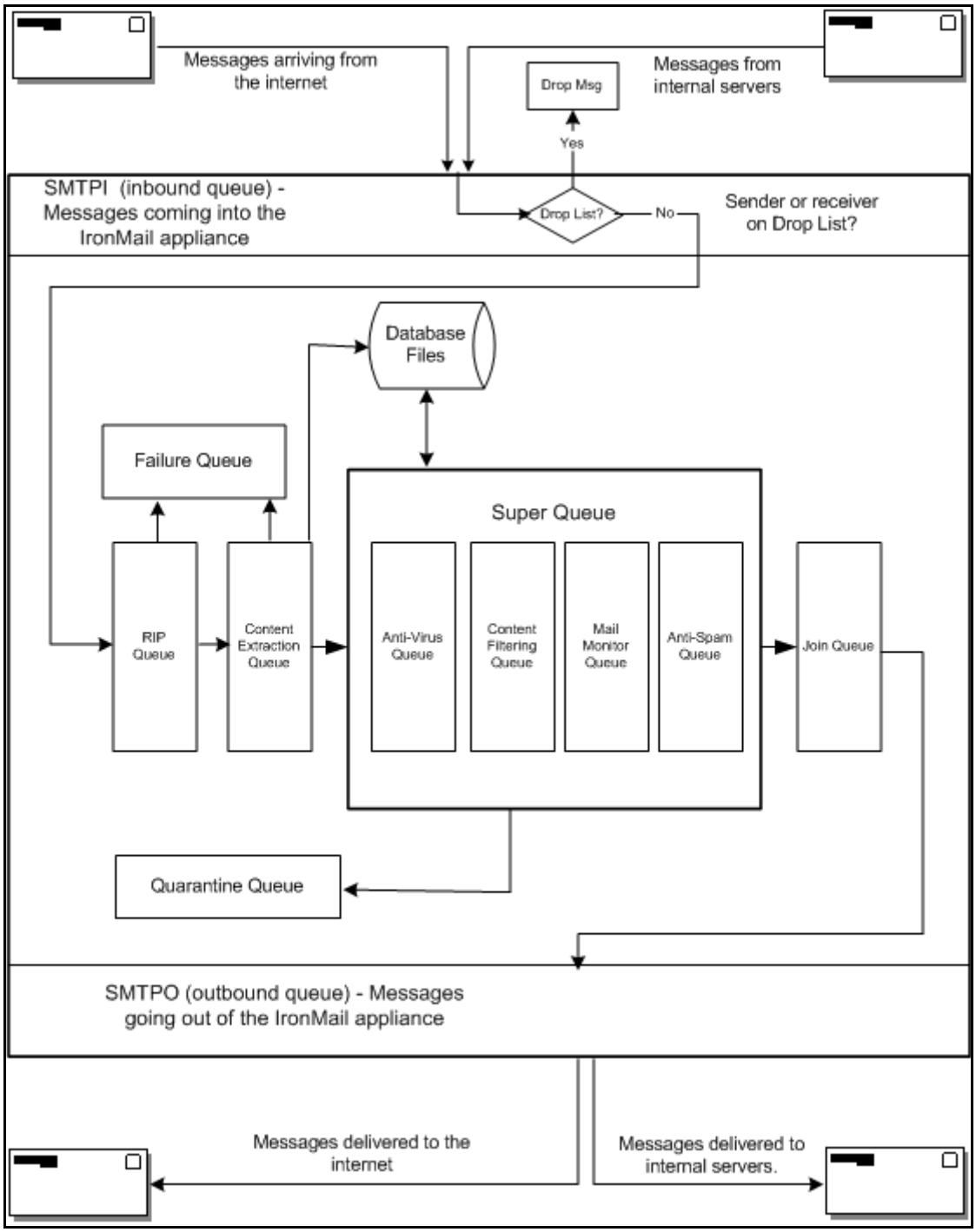
“Queues” are a core component of IronMail’s functionality. IronMail’s queues, while not physical entities like disk partitions, are subsystems that process messages in an ordered fashion. After IronMail’s SMTPI Service receives a message, it passes it to the first subsystem, or queue, in line. Each queue “wakes up” at periodic intervals to see if new messages are ready for it to process. After each queue subsystem finishes processing the message, it passes it on to the next queue in line. Each queue is designed to perform very specific tasks. Once all queues have processed the message, IronMail’s SMTPO Service delivers it to its final destination—assuming that a queue did not have to quarantine, drop, re-route, or take some other action on the message.

For additional information and configuration procedures for queues, see the Queue Manager section of this manual.

IronMail's former queue structure routed messages through the processes as shown in the diagram below:



That flow of messages has been replaced by the creation of a SuperQueue, as shown:



Initial Queues

IronMail uses two queues that are visible to administrators on the Queue Information screen, but there are no hyperlinks to open these queues to view the details of how messages are being processed within them. Administrators can only see the number of messages being processed within the queues. These queues include the following:

- Rip Queue
- Content Extraction Queue

The **Rip Queue** is the first to process an email, and its task is to "rip" the message into its constituent *MIME* parts. Rip Queue writes the *original* message to disk, and enters copies of the message parts as part files, and references to the part files in an internal database. Each subsequent queue examines the message parts.

The **Content Extraction Queue** processes messages before they are examined in the SuperQueue. The Content Extraction Queue runs right after the Rip Queue, and converts proprietary text files (e.g., Word docs) into an ASCII text format that IronMail can "read" for the purpose of enforcing policies such as those configured in Content Filtering (dictionaries) and Attachment Filtering.

Note: Some caution is required when an Administrator creates rules (e.g., in Attachment Filtering) due to the functioning of the Content Extraction Queue. If you create a *rule* with certain extension types (.scr, .pif, .sea), Content Extraction will see them not as the extension types specified, but as .exe attachments. If the rules in place are intended to allow .exe attachments, but to capture any of the other specific extension types, the rules may not function as intended. In the example cited, the three types listed would pass through Attachment Filtering because they would be seen as .exe files; the file extensions (.scr or .pif) do not indicate that the files are not executabes. More information is available at *Policy* Manager > Attachment Filtering > Attachment Filtering and Content Extraction.

The SuperQueue

While previous versions of IronMail used separate queues for the various features to process messages, four features within one queue, the SuperQueue, process messages between the Rip Queue and Join Queue. These features are visible and configurable by the IronMail Administrator:

Anti-Virus Scanning uses the configuration settings in the Anti-Virus program area of IronMail when it processes messages in its queue. The Anti-Virus Scanning feature performs all the actions configured in *Anti-Virus > Configure Anti-Virus*. Additional options may be configured by clicking the "Queue – Virus Scan" hyperlink in *Queue Manager > Configure Queues*.

Content Filtering enforces the Attachment Filtering, Message Stamping, and Content Filtering policies created in IronMail's Policy Manager. (The Content Filtering feature performs its tasks according to the following precedence rules: first it enforces the Attachment Filtering policies, then it enforces the Content Filtering policies, and last it enforces the Message Stamping policy.) Additional options may be configured by clicking the "Queue – Content Filtering" hyperlink in *Queue Manager > Configure Queues*.

Mail Monitoring enforces the Off-Hour Delivery, Mail Monitoring, and Encrypted Message Filtering policies created in IronMail's Policy Manager. (The Mail Monitoring feature performs its tasks according to the following precedence rules: first it enforces the Encrypted Message Filtering policies, then it enforces Mail Monitoring, and last, it enforces Off-Hour Delivery.) Additional options may be configured by clicking the "Queue – Mail Monitoring" hyperlink in *Queue Manager > Configure Queues*.

Anti-Spam uses a variety of anti-spam tools configured in IronMail's Anti-Spam program area to inspect messages for characteristics of spam. When a message is found to be spam-like, an administrator-defined action (e.g., drop, quarantine, rename, etc) is performed on it. Additional options may be configured by clicking the "Queue – Anti-Spam" hyperlink in *Queue Manager > Configure Queues*.

Non-Processing Queues

IronMail also includes two other queues that do not actually process messages, but that are used to store them under specific conditions. These queues are:

- The Quarantine Queue, and
- The Failures Queue.

Quarantine Queue

The **Quarantine Queue** is not a message-processing queue, but rather a logical "holding area" where other queue services may send message if certain conditions are met. Whereas the other queues and features actually process messages in some way, the Quarantine Queue is completely passive. Some of Policy Manager's rules have a "send to Quarantine" action if certain message characteristics are found. Additionally, large emails held for Off-Hour Delivery are stored here. IronMail's Queue Manager allows administrators to create multiple quarantine queues to facilitate the management of its email policies. The administrator may view the contents of the quarantine queues at any time (through a search function). The administrator may delete, re-prioritize, change the scheduled delivery time, or re-direct to an alternate address any message in any of the quarantine queues.

Failures Queue

The **Failures Queue** is used if a message fails Rip, Contract Extraction, or Join Queue processing. Messages generally end up in the Failures Queue because of an inability to parse message attachments or to extract text content, or because of a Join Queue quarantine action. The specific actions taken for messages in the Failure Queue depend on options defined from the Configure Queues screen in the Queue Manager.

MIME Parse Failures

All messages (messages NOT generated by IronMail) pass through the RIP Queue. The RIP Queue parses the messages into individual parts both in the disk as part files and also in the database as references to the message parts.

Each subsequent queue examines the message parts within the database.

Sometimes a message fails Rip Queue or Content Extraction Queue processing (the message cannot be broken into its component parts). In the event of a *MIME parse failure*, the message does not pass through the Content Filtering feature. As a result, Attachment Filtering, Content Filtering, and Message Stamping features are not available for messages with MIME parse failures. However MIME parse failures can pass through all the queues and features that do not need the email message to be broken down into parts.

When any of the repackage actions are set for messages that are MIME parse failures, the messages pass through all the queues and features that do not need the email message to be parsed as long as the queues are configured. These are:

- Anti-Virus
- Mail Monitoring
- Anti-Spam
- Drop
- Quarantine

For MIME parse failures, four actions are available (Drop Message, Deliver to Recipient, Deliver to alternate address, and Quarantine Message). These actions are specified as the MIME Parse Failure Action on the Configure Queues in the Queue Manager.

Additional considerations also apply in the event of MIME parse issues. For example, if the IronMail RIP queue is able to parse the message into parts but JOIN queue is unable to rebuild the message back from the individual parts for whatever reason, IronMail requires a special configuration. (See the MIME Rebuilding Failure Actions.)

Note: The Secure Web Delivery (SWD) feature also requires the message to have valid MIME. For the messages where RIP queue is unable to parse the message successfully, the SWD option will

not be available. This means the SMTPO process when checking for availability of SWD will also check for validity of the message for MIME.

The Final Queues

The Join Queue

The **Join Queue** is the last to process an email, and its task is to reassemble the message back into a whole. If any of the features within the SuperQueue performed an action—such as rewriting a Subject line or deleting offensive words—the Join Queue deletes the original message from the Message Store, reassembles the message from the IronMail-edited parts stored in the database and delivers it to the SMTPO Service for final delivery, assuming that a feature did not have to quarantine, drop, or re-route the message.

The Outbound Queue

Once a message has passed through all the processing queues without being stopped by a triggered action, it is ready to be sent on to the intended recipient.

The **Outbound Queue** is really IronMail's SMTPO Service, responsible for delivering messages out of the IronMail appliance. The terms "SMTPO Service" and "Outbound Queue" are used interchangeably. IronMail's SMTPO Service wakes up at periodic intervals to see which messages have been processed by all the other queues. The administrator may view the contents of the Outbound Queue—that is, view the messages ready for delivery, but not yet delivered—and re-prioritize the delivery of either individual messages or all messages addressed to a specific domain, or delete them.

The queues perform their tasks on messages sequentially. That is, messages do not enter a new queue until they have successfully passed out of the previous one. Administrators may specify the order or sequence in which the queues process messages (*Queue Manager > Configure Queues*).

IronMail can only scan a maximum of 500 message parts. If a message contains 501 or more parts, IronMail will respond with a "MIME Parse Failure" and perform the action specified in the MIME Parsing Failure Action input field of the Global Properties (*Queue Manager > Configure Queues > Global* hyperlink).

Queue Information, Configure Queue, Outbound Queue, Search, Domain Priority, and Quarantine Type sub-menus in the left navigation frame of the Web Administration interface offer a variety of tools for managing messages within IronMail's queues.

Inside the SuperQueue

SuperQueue is a single queue that is responsible for the features of IronMail, including the following:

- Anti-Virus
- Mail Monitoring
- Encrypted Message Filtering
- Off-Hour Delivery
- Attachment Filtering
- Content Filtering
- Message Stamping
- Anti-Spam

Instead of spinning a separate channel for each message to be processed, SuperQueue has a pool of channels that are always alive. One SuperQueue function will assign messages to each channel.

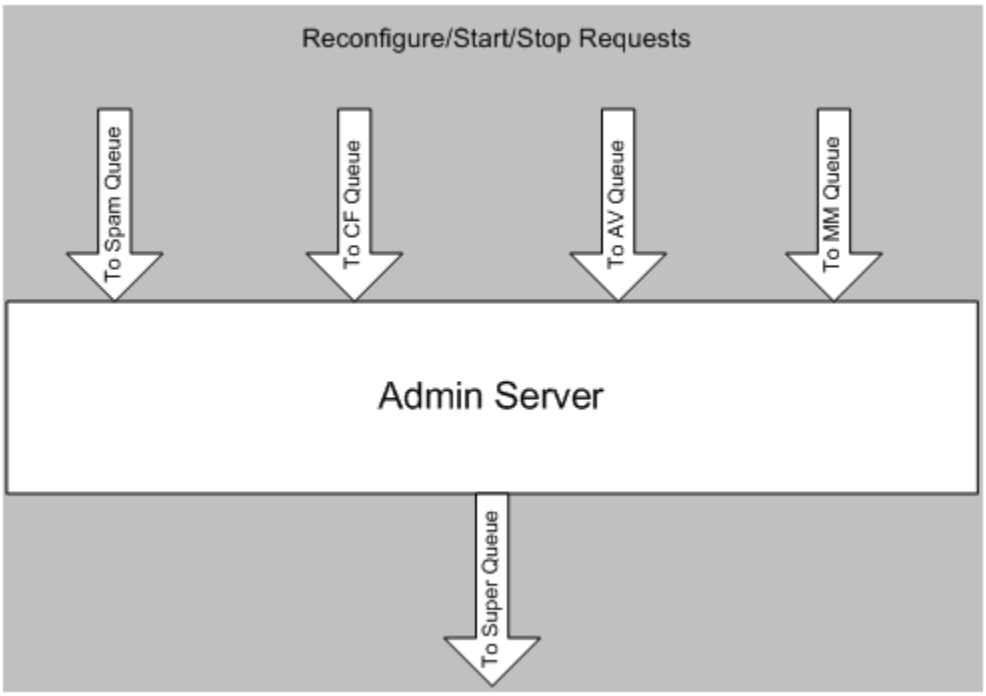
Major advantages and disadvantages to implementation of the SuperQueue are summarized in the following table.

Advantages	Disadvantages
Polling of the database is reduced to 25% from polling by individual queues. Wait time for each message is reduced to the wait time for one queue rather than four. Each channel owns a database handle by itself, reducing database handle contention. Common activities, such as group identification, are done only once rather than individually by each queue. Inter-queue communication is more flexible. Identification and logging of processing actions for each message is easier.	There is one large, bulky process rather than four smaller ones. ST mode failure handling requires increased intelligence. If a message is stuck in a queue, the process must consider what features have already completed processing the message and which have not, in order to avoid repeating processes unnecessarily when the queue is stopped and restarted by "watch."

The SuperQueue includes three major functional components: QServer, QSpinner, and QChannel. The user interface (GUI) is the method for communicating with SuperQueue and its components.

GUI Administration

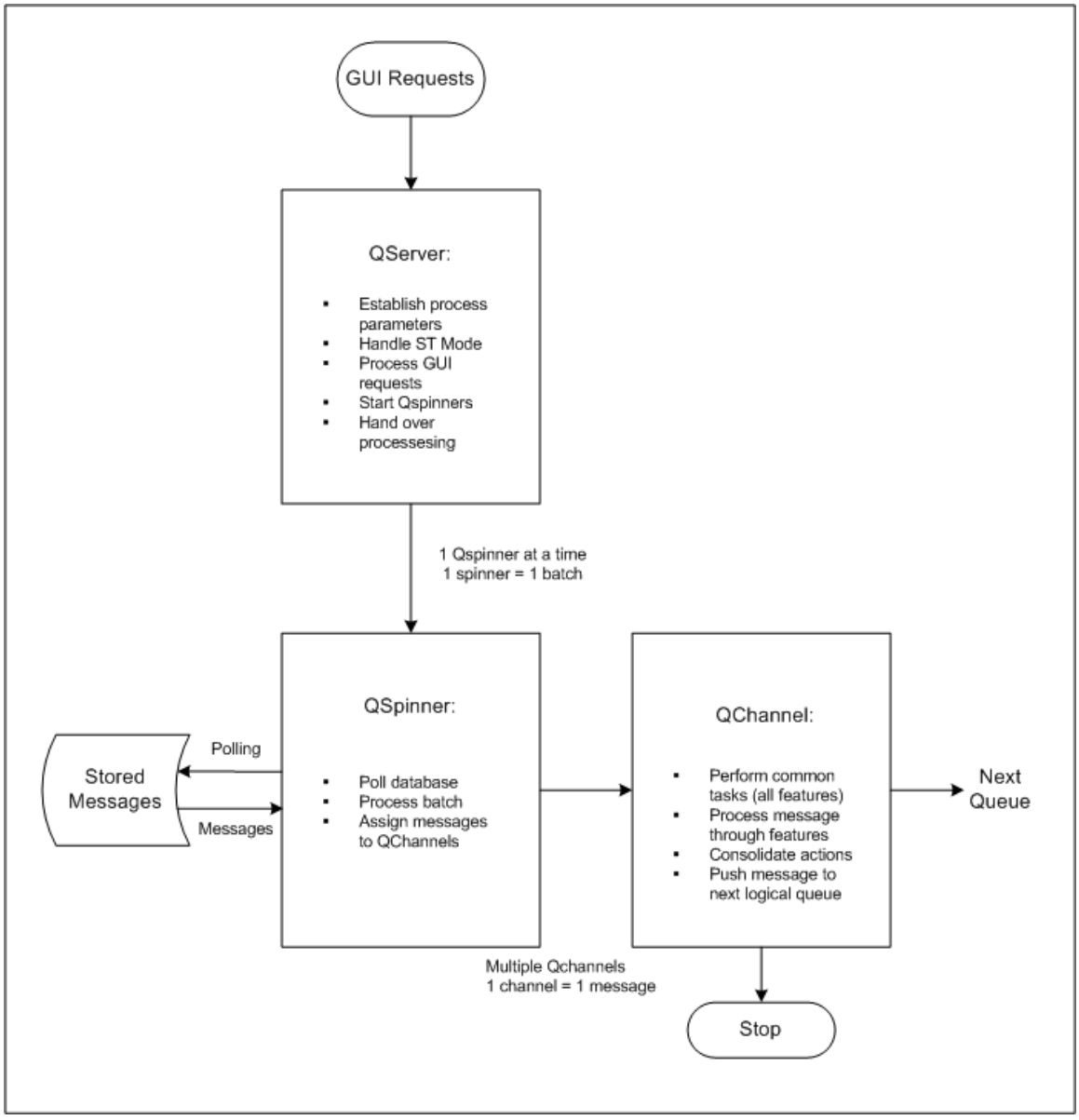
The user or Administrator sends configuration settings and changes and other commands to the SuperQueue from the GUIs for the specific features. However, the Admin server is configured to send reconfiguration commands, etc., to the SuperQueue instead of the individual features. From the user's point of view, the changes are mostly transparent.



SuperQueue Functions

SuperQueue Flow

A high-level overview of SuperQueue's flow is shown in this diagram.



Greater detail about each of the functions is included below.

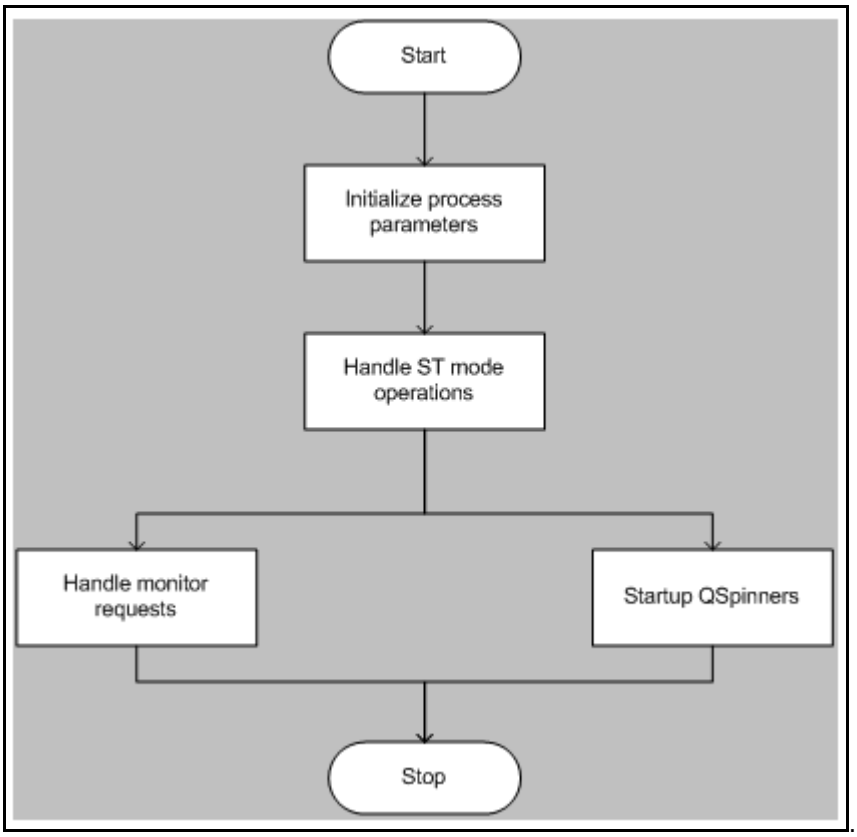
QServer

QServer is the main thread in the SuperQueue, and is responsible for the following actions:

- Initializing all the process parameters - reading the parameters from the database and initializing a set of QChannel instances. QServer will create a pool of the QChannel instances that will be waiting to process messages.
- Handling Single-Thread (ST) Mode operations - handling the processing for those messages that were under process when the previous instance of the queue died.
- Monitoring requests - handling all monitor port requests, such as reconfig, dumpstat, hardstop, softstop, etc. The reconfig command for the SuperQueue will support the individual reconfig commands for the included queues.
- Starting QSpinner - creating a new QSpinner instance at regular intervals (every three seconds) and handing processing over to that instance. A new QSpinner instance is

created only when the previous instance has completed its processing. One QSpinner will retrieve and process one batch of messages.

QServer's functions are illustrated in the following diagram.

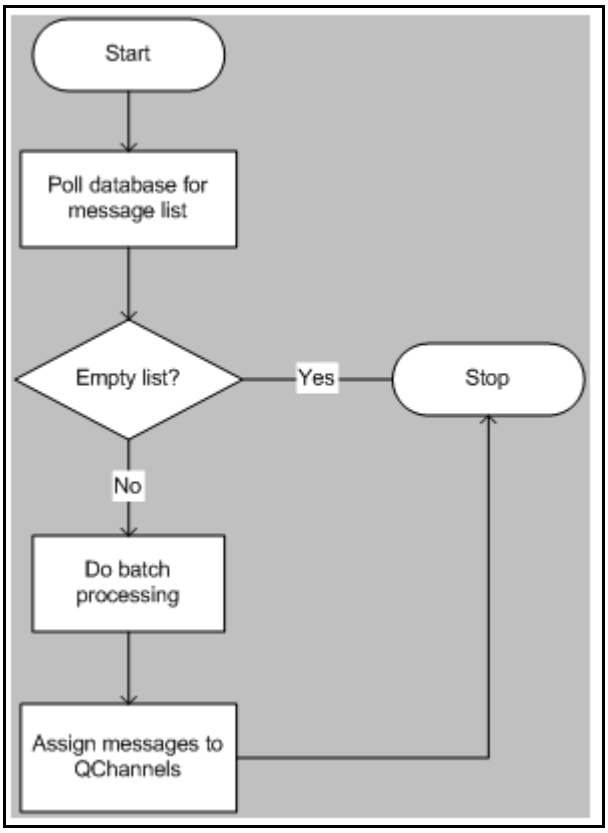


QSpinner

QSpinner is the intermediate thread between the main thread and the actual processing thread. It is responsible for the following actions:

- Polling the database - getting a list of messages to be processed (one batch). At the beginning of each run, QSpinner retrieves the message list from **`ct_msg_heap`**; other characteristics of the message are retrieved from **`ct_message`**, **`ct_message_part`** and **`ct_action`**.
- Batch processing - performing activities that are common to each message for groups of messages, that would consume time and resources if done for each message individually (e.g., SLS lookups).
- QChannel handling - assigning each of the messages in the list to individual QChannel instances as they are freed. QSpinner waits for a free channel and then assigns a message to it. One QChannel will handle one message.

The diagram below shows QSpinner's process flow.

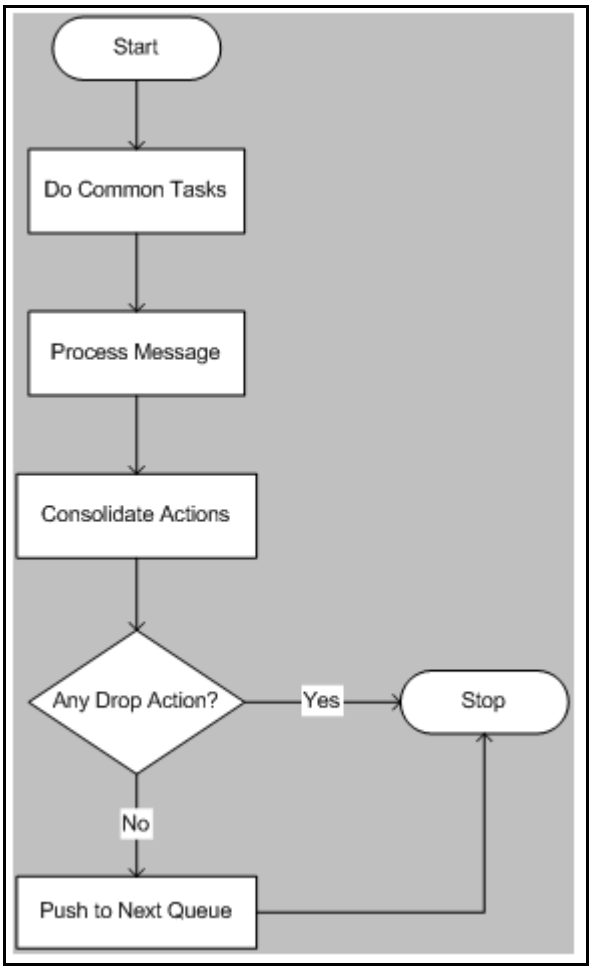


QChannel

QChannel is the thread that actually processes the message. A pre-determined number of these channels will constitute the pool created by QServer, and will process messages as assigned by QSpinner. QChannel is responsible for the following:

- Common tasks - performing tasks that will be used by the individual sub-queues, such as getting detailed information for the message and its individual parts, and getting group information for the message.
- Message processing - performing the actual processing of each message for the enabled features. The features may include Anti-Virus, Mail Monitoring, Anti-Spam and Content Filtering, each of which constitutes a bucket called as a sub-queue. The messages are processed by the sub-queues sequentially, in the order configured by the Administrator.
- Consolidating actions - consolidating the actions triggered by the individual policies and rules for the sub-queues. QChannel will apply the precedence of the various actions while it is consolidating.
- Pushing messages to the next queue - after all processing and consolidation, sending the message to the Join Queue (the next logical queue). The message will be pushed only if no drop action has been triggered.

QChannel's flow is illustrated in the diagram.



Managing Policy

Policy Manager

IronMail allows a broad range of "policy management" capabilities. That is, once IronMail accepts messages based on the SMTPI settings, there are a great many conditions that can affect how IronMail should ultimately process them. From altering message "header" information, to "content filtering," to processing large emails, the tools here give administrators the ability to create a variety of "policies" controlling email usage in the *network*.

Every time a message is received by IronMail's SMTPI Service, an internal "lookup" is performed to determine which policies are to be enforced on it. The policies in effect as of the moment the message arrived at the appliance are enforced. Once a message is received for processing, subsequent changes made to IronMail's policies do not apply to that message. Changed policies only affect new messages entering the IronMail appliance after the *policy* was updated.

Policy management is a licensed feature of IronMail. Unless a Policy Manager license has been purchased and installed on the appliance, this program area is completely removed from the Web Administration interface.

Queue Whitelist, Address Masquerade, Group Manager, Mail Monitoring, Encrypted Message Filtering, Off-Hour Delivery, Attachment Filtering, Content Filtering, Message Stamping, Mail Notification and End User Quarantine hyperlinks in the left navigation frame allow configuration of IronMail's email policies.

Note that when IronMail reports statistics about the numbers of messages it processed, and which messages were affected by an email policy, there may be discrepancies between the total count and sub-total counts of messages in IronMail's Daily Reports. This is because IronMail's Queue Services do not necessarily examine every message. For example, if the Content Filtering Queue was the first to examine a message, and sent the message to a quarantine queue as a result of the policy, the message might never be examined by the Anti-Spam Queue. Or if the Content Filtering Queue notes that a message contains a large number of file attachments and the message is ultimately dropped, those attachment file-types may not be represented in IronMail's SMTPO Outgoing Daily Report. The result of enforced email policies, and the order in which IronMail's Queue Services process messages, all impact the data recorded in IronMail's Daily Reports.

Creating IronMail Policy

Creating IronMail policies requires two steps.

- First, administrators must create a *rule* specifying what messages IronMail should be on the lookout for.
- And second, they must apply the rule to individuals or a group of users. Rules are inactive until they are applied.

Each feature in the *Policy* Manager program area provides the Administrator with the opportunity to configure policies for the enterprise.

Note: In network configurations that use a Consolidated Quarantine Server (CQS), the processing order, rules and policies must be configured the same way on all IronMail appliances. If this is not done, the CQS will not function properly.

Queue Whitelisting

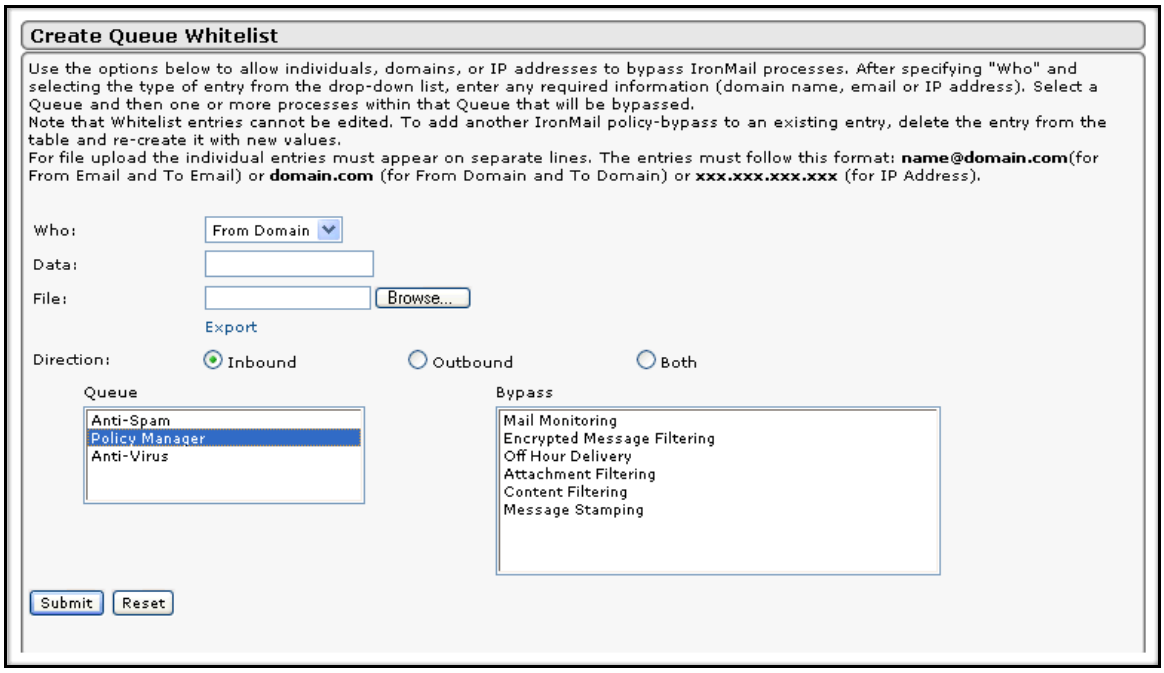
Queue Whitelist

The Queue Whitelist program area allows administrators to finely differentiate which users or domains may bypass any or all of IronMail's *policy* and queue services. In this way, for example, "trusted groups" of users may be allowed to bypass the Content Filtering Queue's Attachment Filtering policies or the Anti-Spam Queue's Statistical Lookup Service inspection. The Queue Whitelist allows differentiation between inbound and outbound messaging.

The Queue Whitelist hyperlink expands to offer Create, Search, View and Apply sub-menus.

Create Whitelists

The Create Queue Whitelist page allows the creation of "Whitelist rules." Enter individual email addresses, domain names, or IP addresses, and for each, indicate if the *rule* for those entities applies to inbound or outbound messages, and which IronMail policies those messages may bypass.


Create Queue Whitelist
Use the options below to allow individuals, domains, or IP addresses to bypass IronMail processes. After specifying "Who" and selecting the type of entry from the drop-down list, enter any required information (domain name, email or IP address). Select a Queue and then one or more processes within that Queue that will be bypassed.
Note that Whitelist entries cannot be edited. To add another IronMail policy-bypass to an existing entry, delete the entry from the table and re-create it with new values.
For file upload the individual entries must appear on separate lines. The entries must follow this format: name@domain.com(for From Email and To Email) or domain.com (for From Domain and To Domain) or xxx.xxx.xxx.xxx (for IP Address).
Who:
From Domain
Data:
File:
Browse...
Export
Direction:
Inbound
Outbound
Both
Queue
Anti-Spam
Policy Manager
Anti-Virus
Bypass
Mail Monitoring
Encrypted Message Filtering
Off Hour Delivery
Attachment Filtering
Content Filtering
Message Stamping
Submit
Reset

IronMail will automatically convert whitelist entries to lowercase letters.

Note: When determining if a message may bypass a queue or *policy*, IronMail will look for the specified address in the message's RFC821 header. If the Administrator enters data obtained from a message's RFC822 header, and that data is different from the RFC821 header, then email to or from that domain or address may not bypass the selected queues or IronMail policies.

Who	The "Who" column identifies who is allowed to bypass a specific Queue. From the **Who** pick list below the table, select: • **From Domain:** all messages that originate from a specified domain (e.g., mydomain.com) may bypass a queue. • **To Domain:** all messages addressed to a specified domain (e.g., mypartner.com) may bypass a queue. • **From Email:** all messages from a specified email address (e.g., david@domain.com) may bypass a queue. • **To Email:** all messages addressed to a specified email address (e.g., tangela@domain.com) may bypass a queue. • **IP Address:** all messages addressed to or originating from a specified *IP address* or *subnet* (e.g., 121.198.17.8, 121.198.17) may bypass a queue.
Data	Enter in the **Data** input field below the table information relevant to the "Who" specified above. For example, enter a valid email address if To Email or From Email was specified. Enter a *domain name* if To or From Domain was selected. Enter a specific IP address or subnet if this was selected above. Note that only class A, B, and C subnets are allowed.

File	Importing a whitelist cannot be performed "globally"—i.e. a single list of all domains, email and IP addresses from another source cannot be imported into IronMail. Because IronMail provides so many bypass options (inbound, outbound, granularity of queues and policies to bypass, etc.), a comprehensive list of addresses must first be broken into smaller lists based on address-type and bypass options. For example, a list of all email addresses allowed to bypass Content Filtering may be successfully imported. And a single list of domains to bypass all Anti-Spam evaluation may also be imported. But select policies cannot be applied to one set of addresses on a list, while different policies are applied to yet another group of addresses in the same list.
	
	The import file should contain one or more lines in the following format:
	`type|direction|data|anti_spam_bypass|policy_manager_bypass|anti-virus_bypass`
	
	Where **type** is a required field and must contain one of the following values (without the quotation marks): "from domain", "to domain", "from email", "to email", or "ip address". (The names are case insensitive.) *Where* "direction" is a required field and must contain one of the following values (without the quotation marks): "inbound", "outbound", or "both". (The names are case insensitive.)
	Where **data** is a required field and should contain valid domain, email, or IP address information. *Where* **anti_spam_bypass**, **policy_manager_bypass**, and **anti-virus_bypass** all have the format:
	`Feature:Sub-Feature`
	
	Where **Feature** is the numeric value of a Feature (see below)
	Where **Sub-Feature** is the numeric value of a Sub-Feature (see below)

Direction	Select the proper radio button to indicate the message direction for this rule. You may choose: • **Inbound:** messages originating outside the IronMail-hosted *network* will bypass the specified queue. • **Outbound:** messages originating inside the network and addressed to users outside the IronMail-hosted network will bypass the queue. • **Both:** messages coming from as well as going to a specified user or domain. For example, if the domain "mypartner.com" is the specified "Who," all messages coming from that domain will bypass the queue, as well as all messages from inside the network addressed to it. **Note:** If the Administrator creates an "inbound" rule for a user, domain, or IP address, and later creates an "outbound" rule for it, IronMail will automatically change the "Where" value to "Both" and remove the earlier entry from the table.

Queue	Select from the **Queue** list: • **Anti-Virus:** Selecting Anti-Virus will display in the Bypass list immediate below any installed anti-virus engines. If an Anti-Virus License has not been installed on IronMail, Anti-Virus will not appear in this list. • **Policy Manager:** Selecting Policy Manager will display in the Bypass list immediate below all the types of policies that the Mail Monitoring and Content Filtering Queues enforce. If a Policy Manager License has not been installed on IronMail, Policy Manager will not appear in this list. • **Anti-Spam:** Selecting Anti-Spam will display in the Bypass list immediate below all the individual Anti-Spam tools utilized by IronMail. If an Anti-Spam License has not been installed on IronMail, Anti-Spam will not appear in this list. Shift-click or Control-click multiple items in this list; all individual policies, tools, or services controlled by those items display in the Bypass list immediately below. **Note:** Be sure to select one or more queues on the queue list before selecting any contents on the **Bypass** list.
Bypass	The contents of the **Bypass** list change depending on which group of IronMail functionality is selected in the Queue list immediately above. Shift-click or Control-click individual policies, tools, or services that messages may bypass. **Note:** To avoid deselecting queues, select one or more queues on the list before selecting any contents on the **Bypass** list.

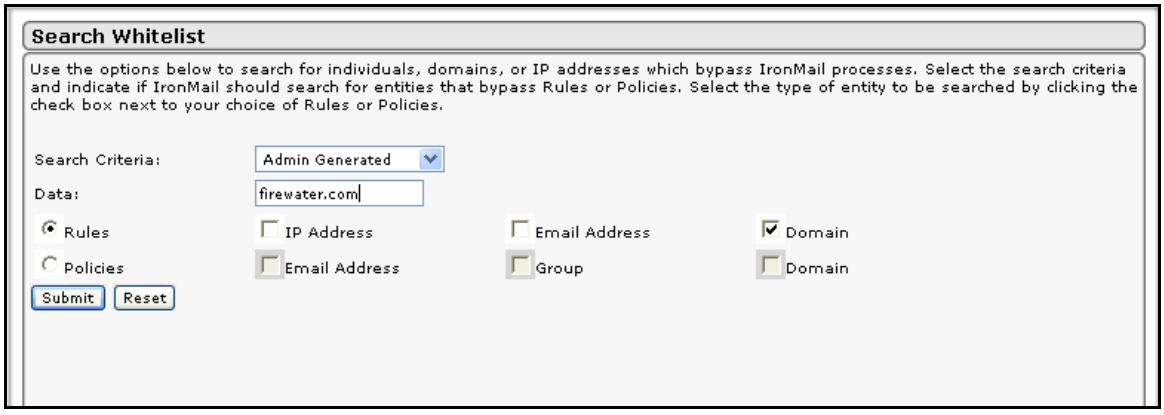
After selecting and entering valid values and information, click **Submit** to create the whitelist rule. Note that Queue Whitelist rules may not be edited. To change a Queue Whitelist rule, delete it from the table and recreate it as desired.

View the contents of the Whitelist by clicking the View hyperlink in the left navigation frame. Remove a Queue Bypass rule by selecting its **Delete** check box and clicking **Submit**. (The **Delete** column heading is also a hyperlink. Clicking **Delete** will select or de-select all rules in the table.)

Important: CipherTrust recommends that whitelists not exceed a total size of 30K, to assure proper functioning.

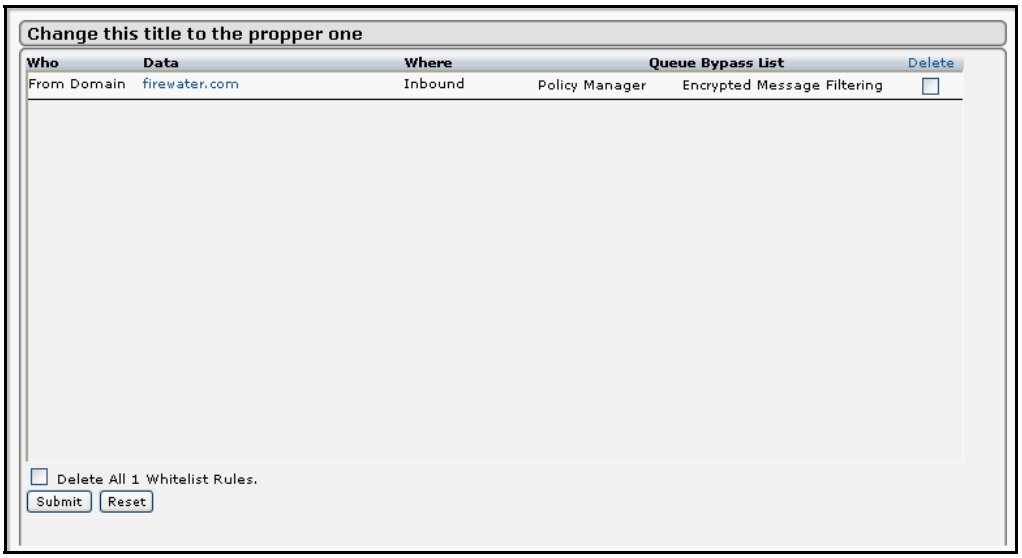
Search Whitelists

Administrators may search for entries in the Whitelist by entering a full or partial email or *IP address*, or *domain name*. There are essentially two types of searches, one based on Rules and the other based on Policies. A *Rule* search seeks to identify the entity that is whitelisted, based on IP address, email address, or domain. A *Policy* search identifies the users, group or domain for which an entity is whitelisted.


Search Whitelist
Use the options below to search for individuals, domains, or IP addresses which bypass IronMail processes. Select the search criteria and indicate if IronMail should search for entities that bypass Rules or Policies. Select the type of entity to be searched by clicking the check box next to your choice of Rules or Policies.
Search Criteria:
Admin Generated
Data:
firewater.com
Rules
IP Address
Email Address
Domain
Policies
Email Address
Group
Domain
Submit
Reset

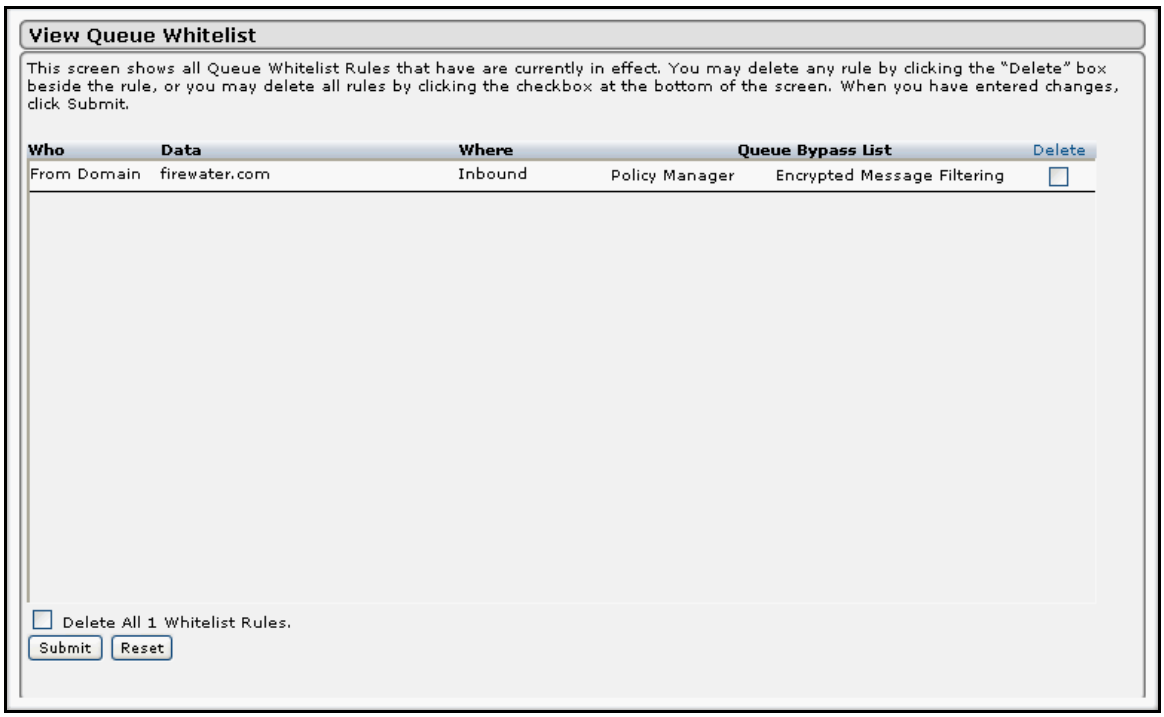
Field	Description
Search Criteria	From the drop-down list, select "Admin Generated" or "End User Generated" to define the type of whitelist entry you wish to find.
Data	In this field, enter any information required for the target of the search (IP address, Group Name, Domain Name, Email Address). You may also enter a query based on information such as a user's name. For example, a Policy query for David Scott will return all email addresses and domains that are whitelisted for him.
Rules	If the search is to be based on a specific rule, click the "Rules" radio button, and then select the parameter for which the search is intended. Options are: • IP Address • Email Address • Domain The search will result in a listing of the entity or entities that have been whitelisted based on the parameter selected. The options for the policy-based search will be unavailable when you select "Rules."
Policies	If the search is to be based on a policy, click the "Policies" radio button, and then select the parameter. Options are: • Email Address • Group • Domain The search will result in a listing of users, groups or domains for which an entity has been whitelisted. The options for the rule-based search will be grayed out when you select "Policies."

After clicking **Submit**, the search results are displayed in a viewing window.



View Whitelists

The contents of the Whitelist are displayed in the View window. When one manually navigates to the View page, the *entire* Whitelist is displayed. (Note that as the Whitelist grows, it may take longer for the browser to "paint" the page.) When one arrives at the view page that results from a query for a specific entity (Search Whitelist), only rules for that entity are displayed.


View Queue Whitelist
This screen shows all Queue Whitelist Rules that have are currently in effect. You may delete any rule by clicking the "Delete" box beside the rule, or you may delete all rules by clicking the checkbox at the bottom of the screen. When you have entered changes, click Submit.
Who
Data
Where
Queue Bypass List
Delete
From Domain
firewater.com
Inbound
Policy Manager
Encrypted Message Filtering
Delete All 1 Whitelist Rules.
Submit
Reset

The View page contains a table offering the following information:

Who	This column displays whether the entry in the Whitelist is an email address, *domain name*, or *IP address*, and whether the bypass *rule* applies to messages addressed to or received from that entity.
Data	This column displays the specific email address, domain name, or IP address allowed to bypass IronMail policies.
Where	This column reports the "direction" for which the bypass rule applies: incoming or outgoing.
Queue Bypass List	This column identifies the specific IronMail policies that may be bypassed.
Delete	Select the **Delete** check box and click **Submit** to delete an entry in the Whitelist table. Note that an entry may not be edited. To modify an entry, delete it from the table and re-create a new bypass rule for it.

Whitelist Rules

The Administrator has the ability to apply whitelisting rules using the following screens. The Whitelist *Rule* Application screen displays all rules that have been created and applied.

Whitelist Rule Application
The table below lists all Queue Whitelist Rules that have been created and shows how they have been applied. You may delete an application by clicking the box in the Delete column for the specific application. Click Add New to perform a new application.
Apply ID
Apply To
Exclude
Delete
10
yourdomain.com
X
9
me@myplace.com
Submit
Reset
Add New

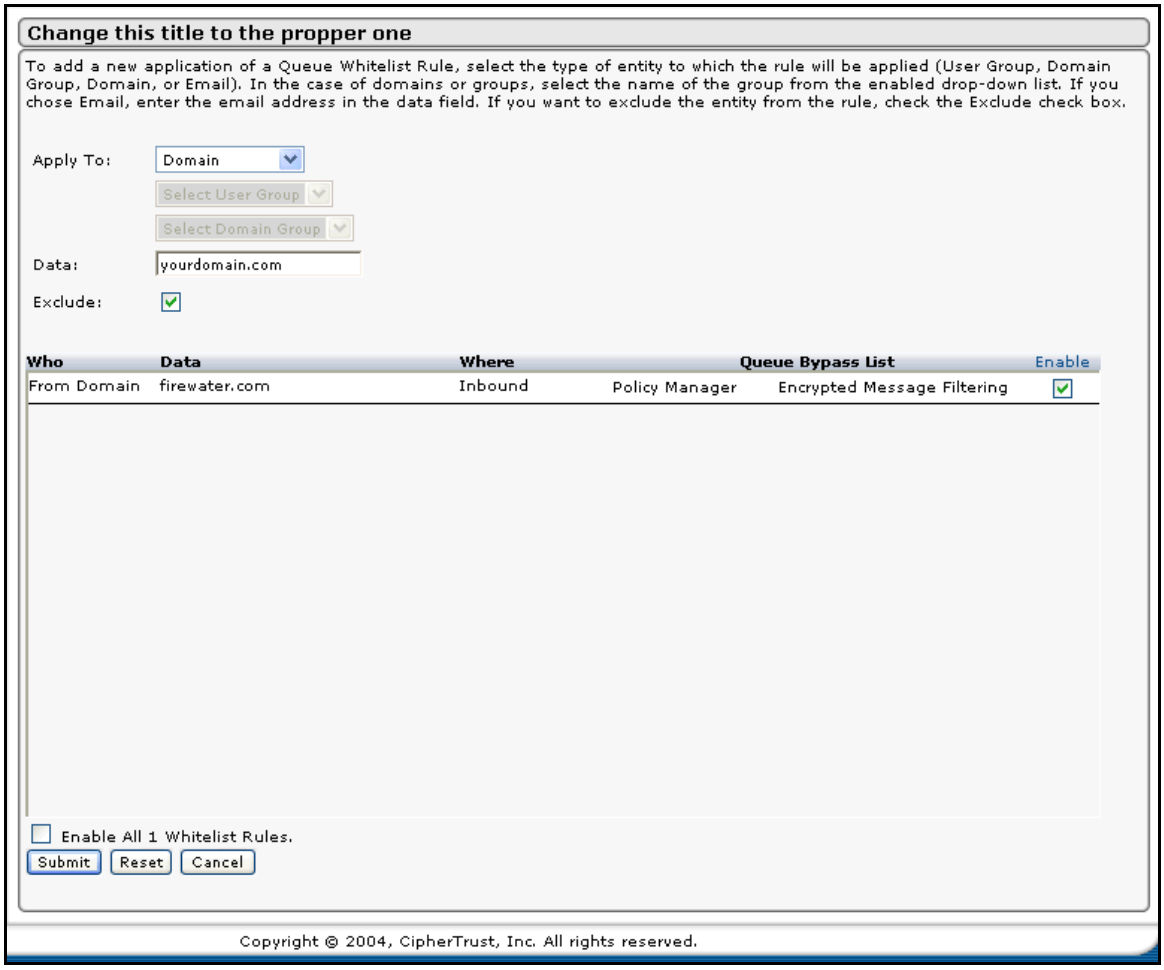
The screen displays the following information:

Field	Description
Apply ID	This column lists the ID number of each application defined by the Administrator
Apply To	The column displays the list of users, groups or domains to which the rules have been applied.
Exclude	If an X appears in this column, the rule is to be applied to everyone except the user, group or domain identified with the rule.
Delete	Clicking the Delete box for any rule will delete that specific application. Clicking the Delete link will allow deletion of all the applications listed.

Click **Submit** to save the applications as shown.

Add a New Rule Application

To add a new application, click **Add New**. The following screen displays.


Change this title to the propper one
To add a new application of a Queue Whitelist Rule, select the type of entity to which the rule will be applied (User Group, Domain Group, Domain, or Email). In the case of domains or groups, select the name of the group from the enabled drop-down list. If you chose Email, enter the email address in the data field. If you want to exclude the entity from the rule, check the Exclude check box.
Apply To:
Domain
Select User Group
Select Domain Group
Data:
yourdomain.com
Exclude:
Who
Data
Where
Queue Bypass List
Enable
From Domain
firewater.com
Inbound
Policy Manager
Encrypted Message Filtering
Enable All 1 Whitelist Rules.
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.

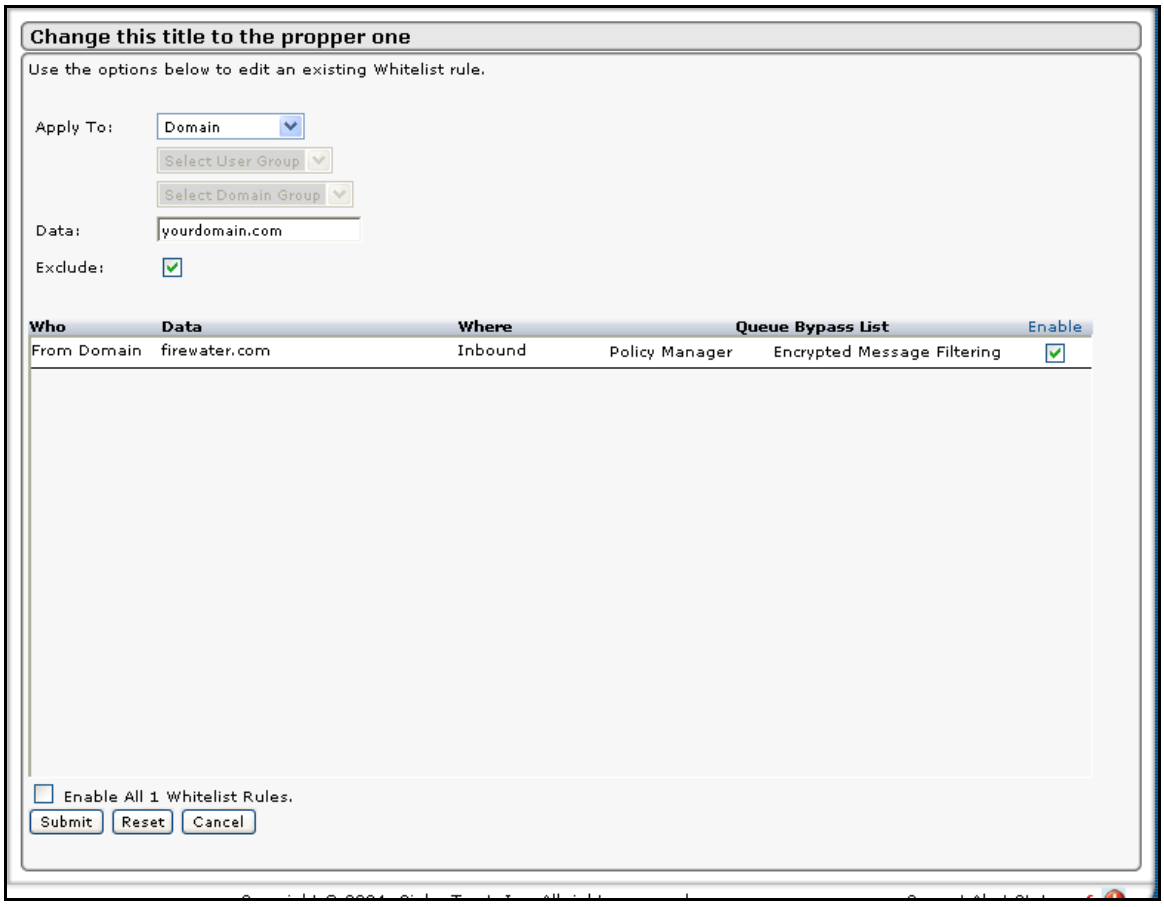
Create a new application of whitelist rules by providing the following information.

Field	Description
Apply To	From the drop-down list, select the type of application to be added. The options for rule application are: • Global - apply the rule to everybody • Domain Group - apply the rule to a group based on domains • Domain - apply the rule to a specific domain • User Group - apply the rule to a group based on individual users • Email Address - apply the rule to a specific email address
Data	Depending upon the selection made for the "Apply To" parameter, select the User Group or Domain Group from the enabled drop-down list, or enter the email address in the Data field.
Exclude	If the rule is intended to apply to everyone except the specific user or group that is identified, click the "Exclude" checkbox.

Existing Rules	***The lower portion of the screen is a table listing the rules that have been created. These rules may be applied by clicking the Enable check box.***
Who	This column displays whether the entry in the Whitelist is an email address, *domain name*, or *IP address*, and whether the bypass rule applies to messages addressed to or received from that entity.
Data	This column displays the specific email address, domain name, or IP address allowed to bypass IronMail policies.
Where	This column reports the "direction" for which the bypass rule applies: incoming or outgoing.
Queue Bypass List	This column identifies the specific IronMail policies that may be bypassed.
Enable	Select the **Enable** check box and click **Submit** to enable the application in the Whitelist table. Note that an entry may not be edited. To modify an entry, delete it from the table and re-create a new bypass rule for it.

Editing an Application

To edit an application, click the Apply ID link on the Whitelist Rule Application screen. And Edit screen displays.



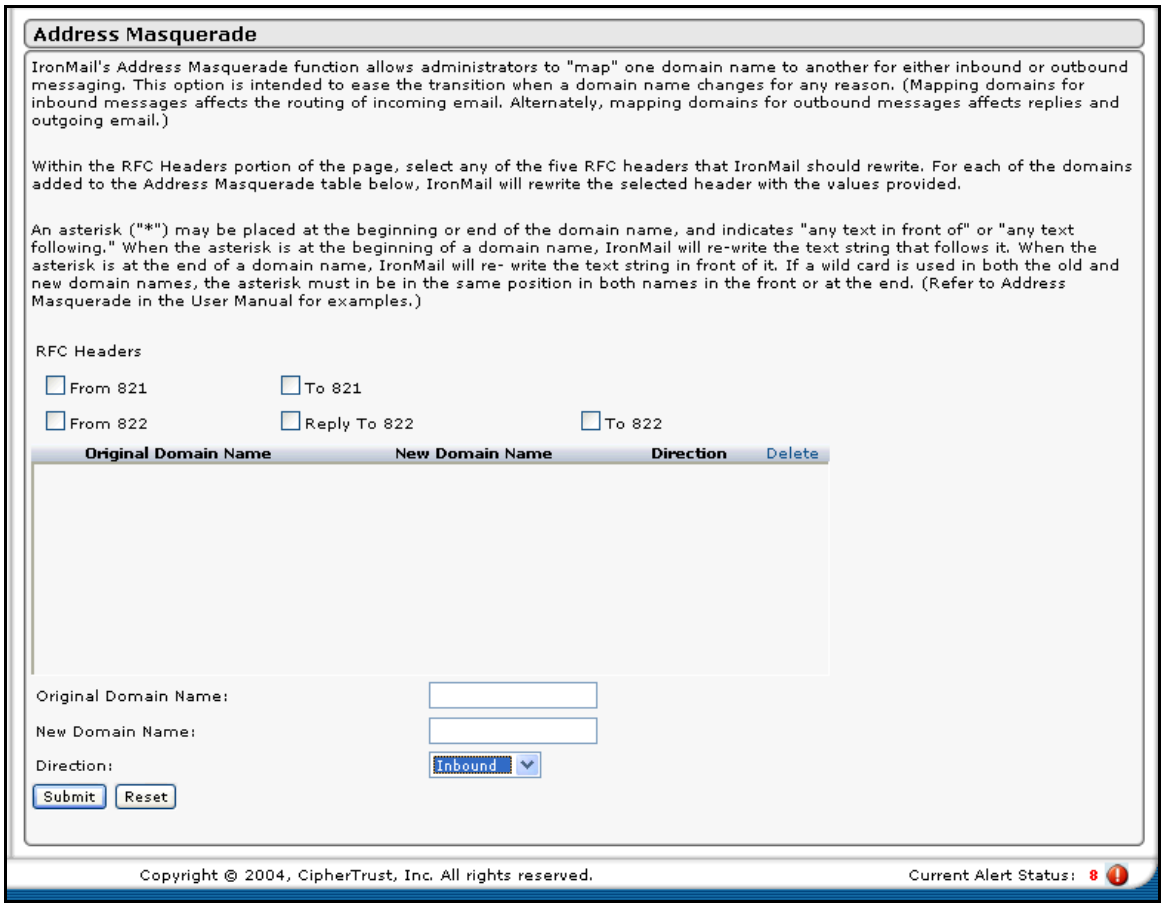
Make any desired changes to the Apply To, Data and Exclude fields, or click the Enable checkbox to toggle the rule on or off. When the changes are complete, click **Submit**.

Note: You cannot change the rule itself from this screen. You may navigate to the View Whitelist screen to delete an existing rule, then go to the Create Whitelist Rule screen and re-enter the rule with new information.

Address Masquerade

IronMail's Address Masquerade function allows administrators to "map" one *domain name* to another for either inbound or outbound messaging. This option is intended to ease the transition when a domain name changes for any reason. Mapping domains on the IronMail appliance protects an enterprise's end users from having to manually change the domain information in their email clients. For example, if "mycompany.com" acquires "yourcompany.com," and wants all mail addressed to "yourcompany.com" to now be routed to "mycompany.com," these two domains would be mapped for *inbound* mail. (Mapping domains for *inbound* messages affects the *routing* of incoming email.) Alternately, mapping domains for *outbound* messages affects *replies* to outgoing email. That is, when "yourcompany.com" is mapped to "mycompany.com," the recipients of outbound messages will see "mycompany.com" as the REPLY TO address.

Note: If a single message contains more than 200 total addresses in the From, To, CC, or BCC headers, IronMail will *not* provide address masquerading for that message.


Address Masquerade
IronMail's Address Masquerade function allows administrators to "map" one domain name to another for either inbound or outbound messaging. This option is intended to ease the transition when a domain name changes for any reason. (Mapping domains for inbound messages affects the routing of incoming email. Alternately, mapping domains for outbound messages affects replies and outgoing email.)
Within the RFC Headers portion of the page, select any of the five RFC headers that IronMail should rewrite. For each of the domains added to the Address Masquerade table below, IronMail will rewrite the selected header with the values provided.
An asterisk ("*") may be placed at the beginning or end of the domain name, and indicates "any text in front of" or "any text following." When the asterisk is at the beginning of a domain name, IronMail will re-write the text string that follows it. When the asterisk is at the end of a domain name, IronMail will re- write the text string in front of it. If a wild card is used in both the old and new domain names, the asterisk must in be in the same position in both names in the front or at the end. (Refer to Address Masquerade in the User Manual for examples.)
RFC Headers
From 821
To 821
From 822
Reply To 822
To 822
Original Domain Name
New Domain Name
Direction
Delete
Original Domain Name:
New Domain Name:
Direction:
Inbound
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 8

Within the RFC Headers portion of the page,

Three input fields below the RFC Headers are used to provide the "mapping" from one domain name to another:

Field	Description
RFC Headers	Select any of the five RFC headers that IronMail should rewrite. The options are: • From 821 • To 821 • From 822 • Reply To 822 • To 822 For each of the domains added to the Address Masquerade table, IronMail will rewrite the selected header with the values provided.
Mapping	***The fields below the RFC Headers are used to map one domain name to another.***
Original Domain Name	This column displays the original domain name which has been mapped to the New Domain Name shown in the adjacent column.
New Domain Name	This column shows the new domain names associated with the domains to which masquerade has been applied.
Direction	Select a direction from the **Direction** pick list for which messages IronMail should rewrite the headers: • **Inbound:** For inbound messages, that is, messages coming into the *network*, the RFC821 TO and RFC822 TO headers should be mapped. • **Outbound:** For outbound messages, that is, for messages addressed to users outside the network, the RFC821 FROM, and RFC822 REPLY TO and FROM headers should be mapped. Note that unless an MX record is created in DNS for the new domain name, message recipients trying to REPLY will be unable to do so. • **Both:** IronMail will rewrite all message headers for both incoming and outgoing messages.
Delete	Checking the Delete checkbox and clicking Submit will delete the associated mapping.
To Add a New Mapping:	***Fields in the lower portion of the table are used to add new masquerade mappings.***
Orignal Domain Name	Enter the original domain name that is to be mapped.
New Domain Name	Enter the new name to which the domain is to be mapped.
Direction	From the drop-down list, select the direction to which the new mapping is to apply.

Click **Submit**. Any new mappings or deletions will be reflected in the upper portion of the screen.

Note that "wild cards" may be used. An asterisk ("*") may be placed at the beginning or end of the domain name, and indicates "any text in front of" or "any text following." When the asterisk is at the beginning of a domain name, IronMail re-writes the text string that follows it; when the asterisk is at the end of a domain name, IronMail re-writes the text string in front of it. If a wild card is used in *both* the old and new domain names, the asterisk must in be in the same position in both names—in the front or at the end.

Examples of address masquerading and wild cards are:

Original or Old Domain Name	Will affect the following domains...	New Domain Name	New name will be...
myoriginalname.com	myoriginalname.com	mynewname.com	mynewname.com
*name.com	myname.com yourname.com hisname.com	*www.com	mywww.com yourwww.com hiswww.com
name.*	name.com name.net name.org	domain.com	domain.com (all the affected domains will become "domain.com")
*trust.com	mytrust.com yourtrust.com ciphertrust.com	*name.com	myname.com yourname.com ciphername.com
trust.*	trust.com trust.net trust.org	name.*	name.com name.net name.org

Note: When using inbound address masquerading, you must create an entry in the Domain-based Routing Table for the "New Domain Name" and ensure that the associated internal mail server is configured to accept mail for the New Domain. If this entry is missing, incoming mail will be rejected with a "571 Cannot relay" error.

Managing Groups

Group Manager

IronMail offers a variety of tools for both creating and enforcing email policy—policies ranging from delaying delivery of large message till off-peak hours, to forwarding or blind copying messages addressed to specific individuals or domains, to disallowing “adult” or “colorful” words in corporate email. These various policies may be applied to individual users, or to groups of users—including domains. The Group Manager program area, therefore, is where administrators may specify or create groups of users for the purpose of *policy* enforcement.

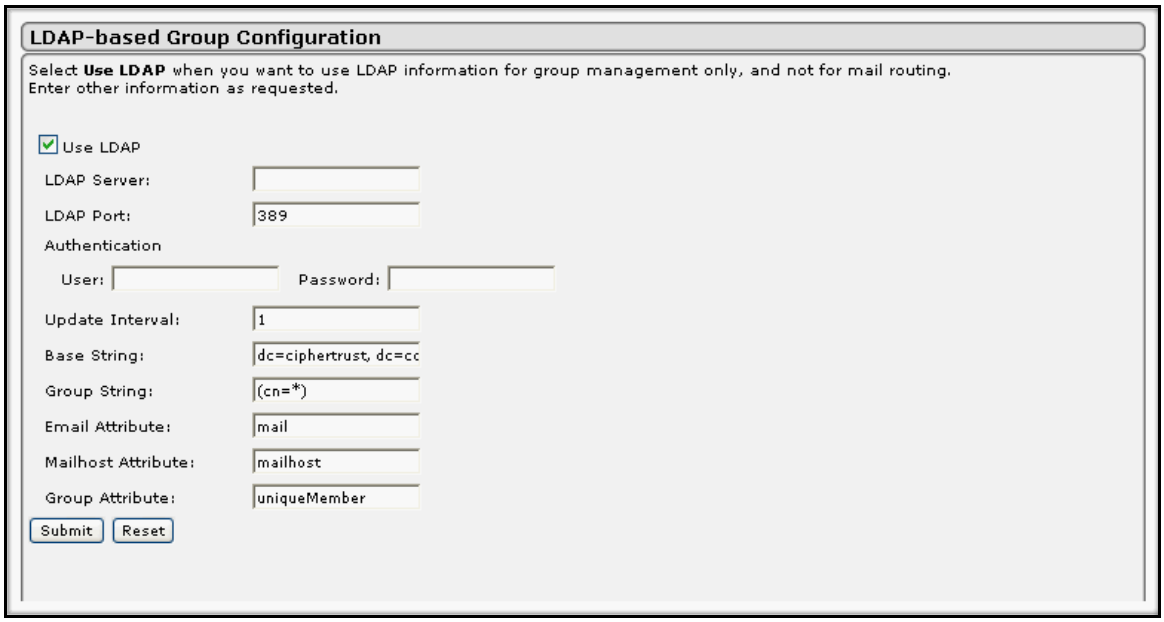
The Group Manager hyperlink in the left navigation frame expands to show LDAP and Definition sub-menus. The LDAP page allows use of group information existing on an external LDAP server. The Definition page allows the manual creation of groups of users, and groups of domains. The Definition screen also allows viewing and editing of LDAP groups.

LDAP

If the **Use LDAP** option is enabled on this page, IronMail will query the internal LDAP server and import the group information it contains. The names of the LDAP groups will display in all of *Policy* Manager’s pick lists that allow the selection of groups of users (e.g. the *Rule* Definition window for the Content Filtering Apply Rule window).

In IronMail 4.5, it is possible to use the LDAP server for both a mail routing task such as "Validate Only," and for synchronizing group information.

Note: When LDAP group information is used, administrators may still manually create groups of users and groups of domains in *Policy Manager > Group Manager > Definition*.



Use LDAP	Check this option to enable to use of the existing group information in an LDAP server for the purpose of applying IronMail policies to groups of users. Mechanism: IronMail queries the LDAP server starting at the "Base String" and requests all the objects specified by the "Group String" (LDAP filter string). The query requests the attribute specified by "Group Attribute." The Group Attribute is usually the "member" or "uniqueMember" attribute. This attribute contains the list of Distinguished Names (DNs) belonging to the group members. IronMail then initiates a second set of queries, this time using each user DN in turn as the new base string. This time, it is requesting the "Email Attribute." This attribute is where the user's email address is stored, and is often named "mail." IronMail then creates groups using the group's Common Name (CN) field populated with the users' email addresses.
LDAP Server	Provides the *IP address* or fully qualified *host name* of the LDAP server.
LDAP Port	The commonly-known default port for non-secure LDAP is port 389. Currently, IronMail does not support LDAP over TLS.
Authentication	Enter the user name and password required to authenticate (bind) to the LDAP directory. The user name should be in the DN format, e.g.: cn=administrator,dc=domain,dc=com. Leave the fields empty to initiate an anonymous bind to the server.
Update Interval	Specify here how often, in hours, IronMail should refresh or synchronize its cache with the LDAP database. The minimum is one hour. **Note:** For large queries or slow connections to the LDAP server, synchronization should be set accordingly. Actual sync times are calculated from midnight. A one-hour schedule will occur every hour on the hour; an eight-hour schedule will occur at midnight and every eight hours thereafter.

Base String	This string defines the point in the LDAP schema where the search begins for group objects. Choosing an appropriate base string can save time and processing resources. It is best to specify the exact branch where the groups exist rather than simply specifying the top level of the directory. Example: ou=groups,o=CipherTrust is better than simply o=CipherTrust. If the groups are not conveniently all in one OU, traverse up the directory to the point in the schema that the groups have in common. Us the group string to ensure that only group objects are returned.
Group String	This LDAP feature string is used to return the group objects that you want to synchronize to IronMail. It should be chosen to return only group objects. Any valid LDAP filter string is allowed, including wildcards. If all the groups were in a single OU and the OU contained only group objects, the Group String could be simply: (objectClass=*) or (cn=*). The following example would retuern only group objects that have the string "admins" in the Common Name attribute. (&(objectClass=groupOfNames)(cn=*admins*)) **Note:** The conditional elements AND (&), OR (|) and NOT (!) are placed after the first parenthesis, and are followed by each condition enclosed in parentheses. A final parenthesis closes the statement.
Email Attribute	Enter the name of the attribute that identifies a user's email address in the LDAP database.
Mailhost Attribute	This attribute is used to check if a valid return is received. The data returned for this attribute serves no other purpose. An example of an attribute that may be used is the "objectClass" attribute as it exists in all objects.
Group Attribute	The name of the attribute that holds the user entries in the group. Common attributes are "member" or "uniqueMember."

Click **Submit** to save user inputs.

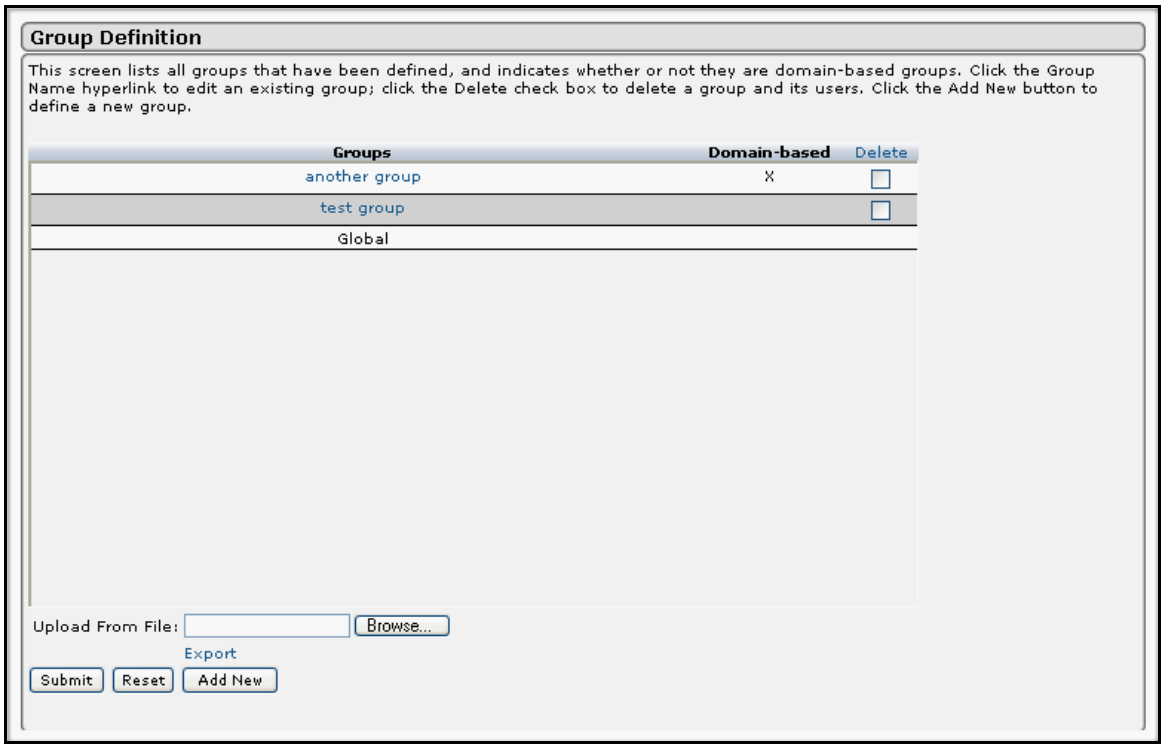
Definition

Use the Group Definition window to manually create groups of users or domains and edit the list of members of groups. The Group Definition table, empty until a group is manually created or imported from an LDAP database, displays the following: group name, an indication that it is a group of domains, and an **Delete** hyperlink to remove groups.

Groups, based on type, may include email addresses or domain names, but not both.

Once the groups have been synchronized from the LDAP server, they can be edited in the same way as any manually-created group. If the name of the group is changed, the group will exist independently of the LDAP group that will be synchronized again at the next synchronization interval. Users may be added and deleted from these groups.

Note: If you change the membership of a group but do not change the group name, the group will be overwritten at the next LDAP synchronization.

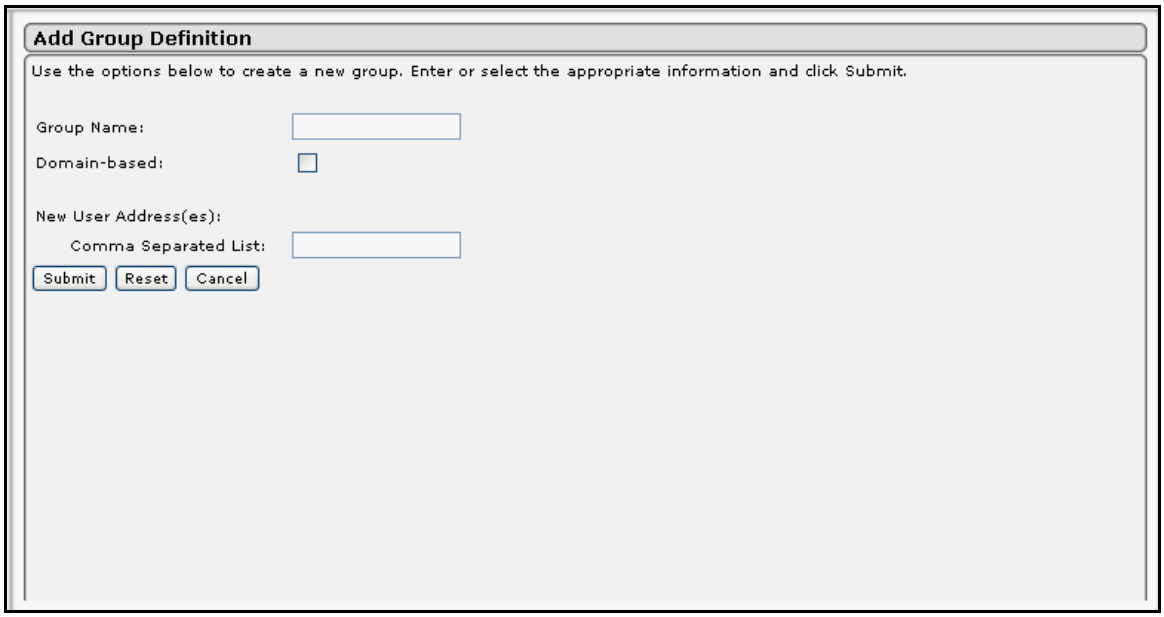

Group Definition
This screen lists all groups that have been defined, and indicates whether or not they are domain-based groups. Click the Group Name hyperlink to edit an existing group; click the Delete check box to delete a group and its users. Click the Add New button to define a new group.
Groups
Domain-based
Delete
another group
X
test group
Global
Upload From File:
Browse...
Export
Submit
Reset
Add New

Field	Definition
Groups	This column lists the groups that have been defined.
Domain-Based	If the group is domain-based, an X in this column indicates this fact.
Delete	Clicking the checkbox for any group will cause that group to be deleted from the screen. Clicking the **Delete** hyperlink deletes all groups. Click **Submit** to carry out the deletions.

Upload From File	Import files for groups are a little different from others. The file may contain more than one group. Each group is defined on a single line of text. Thus, a single file may contain multiple "lists" of groups, with each group being defined in its line. A list of groups in an import file should contain one or more lines in the following format:
	`group_name|domain_based|data_list`
	
	Where **group_name** is a required field and is the name of the group
	Where **domain_based** is a required field that accepts the following values: 0 = User-based Group 1 = Domain-based Group
	Where **data_list** is a comma delimited list of domain names or email addresses (depending on the **domain_based** field value)
	Some good examples of groups are:
	`group1|0|abc@ct.com,dbs@ct.com,snq@hotmail.com`
	`group2|1|abc.com,cde.com,fgh.org`

Adding a New Group

Clicking Add New at the bottom of the screen opens the following screen, allowing the Administrator to define a new group.



You may create groups based on email addresses or domains. That is, groups may contain either email addresses or domain names. (A group cannot contain both email addresses and domains.) When an IronMail *policy* is applied to a group, it affects all the individuals in the group or all members of the specified domains.

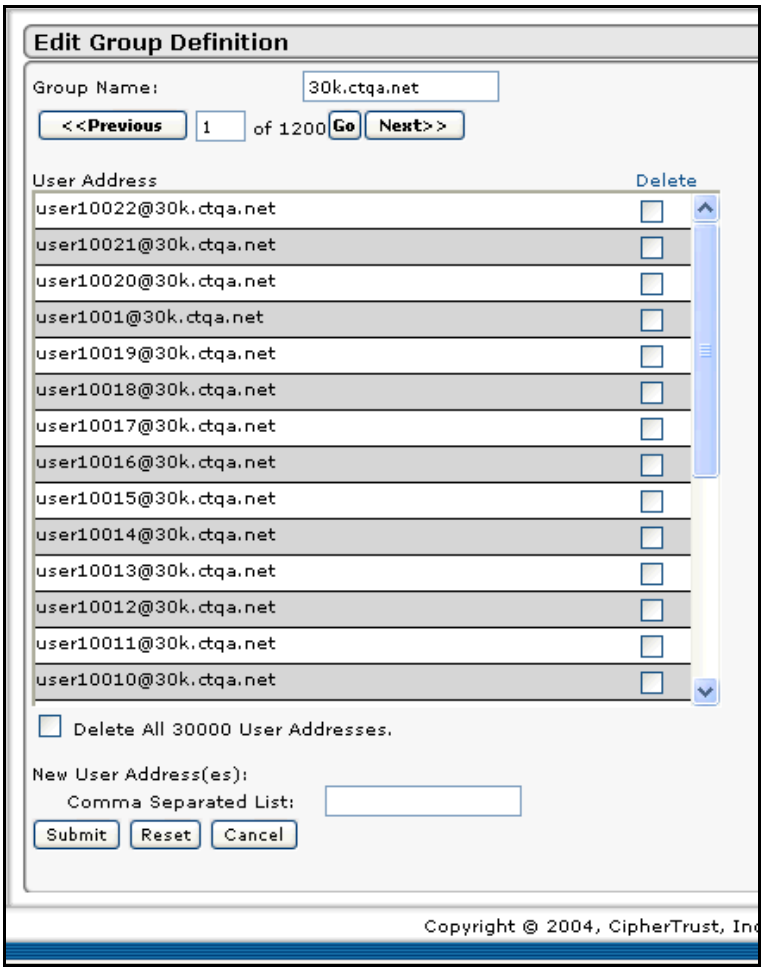
To create a new group, provide the following information.

Groups	Type a descriptive name in this field to identify the new group.
Domain-based	Clicking the check box indicates that the group will consist of domains rather than individual email addresses.
New User Address(es)	Enter the email addresses for all users in the group, or the list of domains for a domain-based group, as a comma-separated list.

Click **Submit** to record the new group. The group information will now appear in the Group Definition screen.

Editing an Existing Group

For any group except "Global," the group name in the Definition screen is a hyperlink. Clicking on the hyperlink allows you to edit an existing group. The following screen displays, allowing you to rename the group, delete addresses from the group, or add new addresses.



The Edit screen contains the following information:

Field	Definition
Group Name	The data field displays the name of the group selected for editing. The group name is editable.
Navigation	Navigation buttons appear if the list of addresses or domains exceeds the maximum allowed for the window. This allows you to move through the addresses or domains one page at a time (**Previous** or **Next**) or to go to a specific page by entering a page number and clicking **Go**.
User Address	This column displays the list of all user addresses or domains that are members of the group.
Delete	Clicking the **Delete** checkbox will delete the specific user address or domain from the group.
Delete All _ User Addresses	Clicking this checkbox will delete the entire list of addresses or domains.
New User Address(es)	To add new users or domains to the group, enter the user address(es) or domain names as a comma-separated list.

Click **Submit** to record all changes.

Monitoring Mail

Mail Monitor

IronMail allows administrators to create policies that monitor specific messages that pass through the email gateway. These "mail monitoring" policies are based on rules that look at every message's sender or receiver email address and check if the email address or domain is identified in a Mail Monitoring *policy*, or if the individual is a member of a group specified in the policy. Mail monitoring policies can alternately be based on a message's Subject lines. IronMail will perform one of ten actions whenever a message whose address/domain or Subject it is looking for is detected.

Mail Monitoring policies are processed in IronMail's *Mail Monitoring* program area. Accordingly, Mail Monitoring must be running in order for Mail Monitoring policies to be enforced. The processing order within the Mail Monitoring feature is illustrated below.

Mail Monitoring Queue				
	Mail Monitoring Policy	**Encrypted Message Filtering Policy**	**Off Hour Delivery Policy**	
From Previous *Queue*	Re-Route - do not proceed to next policy Drop Message - do not proceed to next policy Quarantine - proceed to next policy Secure Delivery - proceed to next policy Forward as Attachment - proceed to next policy Forward - proceed to next policy Subject Re-write - proceed to next policy Copy as Attachment - proceed to next policy Copy - proceed to next policy Log - proceed to next policy	Drop Encrypted - do not proceed to next policy Drop Plain - do not proceed to next policy Quarantine Encrypted - proceed to next policy Quarantine Plain - proceed to next policy Allow - proceed to next policy	Quarantine - - proceed to next policy	*To Next* *Queue*

Some examples of how Mail Monitoring policies are used are:

- When an employee leaves the company, email addressed to him or her may be forwarded to his or her replacement. In this way, important contacts, news sources, and company relationships can be transferred from the old to the new employee.
- If an employee is suspected of using business email improperly, messages addressed to or sent by the individual can be "blind copied" to someone in the Human Resources department.
- If disgruntled individuals repeatedly send email complaints or if they “flame” users within the company, messages from those individuals can be automatically dropped.
- Spam containing the same Subject line can be automatically dropped. For example, holidays will often see an increase in advertisements, and the same spam may be seen over and over again. Mail Monitoring policies based on a message’s Subject line can stop these wasteful messages.

Whenever a message conforms to multiple rules, more than one action may be performed on that message. In some situations, not all actions can be performed.

Policy attribute comparison is used to resolve conflicting actions. In the comparison, a system-defined policy supercedes a user-defined policy, a policy applied to a user supercedes a policy applied to a group, and a higher action code supercedes a lower one.

- If both secure delivery and forward actions could apply to a message, secure delivery has precedence because the forward action could cause the original message to be deleted and the message will not be securely delivered. Other actions can be applied along with secure delivery.

Policy attribute comparison is performed to resolve the conflict above when the actions belong to different policies; just action codes are compared when both rules belong to the same policy.

- When multiple quarantine rules with finite quarantine days may be applied, policy attribute comparison is used to choose one of them. In this case, the quarantine period is compared instead of the action code.

Policy attribute comparison is used between two rules when one of them is either a reroute or drop *rule* to be applied to a sender or subject, or a quarantine forever, and the other rule is an action in (4) or (5). A log action in a policy applied to a user supercedes a reroute action applied to a group.

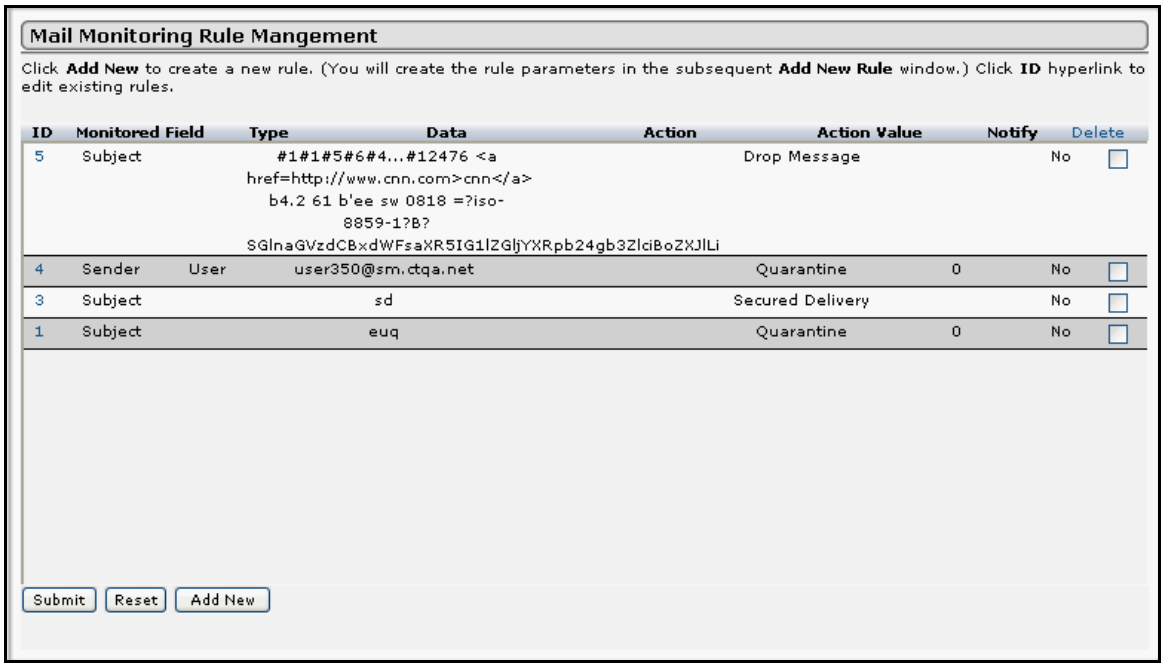
Policy attribute comparison is performed between two rules when either of them is one of the following:

- Reroute rule applied to a sender or subject,
- Drop rule applied to a sender or subject, or
- Quarantine forever.
- If one of the actions is a reroute or drop rule applied to a sender or subject or a quarantine forever, the one action will be performed and all other actions will be ignored because the message will no longer be available for additional actions.

The Mail Monitoring hyperlink expands to offer Manage Rules and Apply Rules sub-menus.

Manage Rules

The Mail Monitoring *Rule* Management table, empty until rules are created, displays information about each Mail Monitoring rule. While individual *rules* are created on this page, they are not "turned into *policies"* until applied to users or groups on the Apply Rules page.



The Mail Monitoring Rule Management table displays the following information:

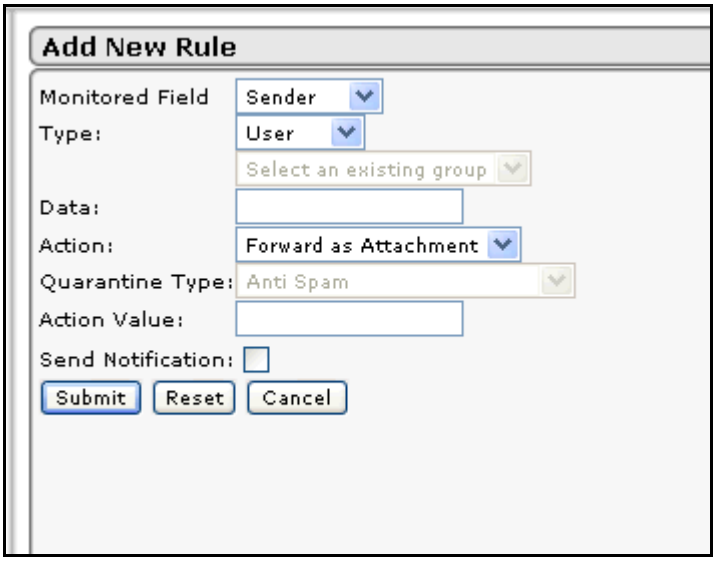
ID	This column displays the unique ID number that IronMail generates for each Mail Monitoring rule. IronMail's logs and reports will report statistics about each rule. Whenever a *policy* is enforced, the report or log will provide information about the message, and the specific Mail Monitoring Rule ID responsible for causing IronMail to act on the message. Rule ID numbers are serially incremented. If a rule is deleted, IronMail does not re-use its ID number. The Rule ID is also a hyperlink opening a secondary browser window in which the rule may be edited.
Monitored Field	This column displays information about which messages will be monitored. One of three values will be displayed: • **Sender:** If the message's FROM address matches the user, group, or domain identified in the **Data** field, IronMail will take the specified action. Messages sent from this or these users will be acted upon accordingly. • **Recipient:** If the message's TO address matches the user, group, or domain identified in the **Data** field, IronMail will take the specified action. Messages addressed to this or these users will be acted upon accordingly. • **Subject:** If the message's SUBJECT line contains the text string provided in the **Data** field, IronMail will take the specified action. Note that the search is a sub-string search. If a Mail Monitoring rule is set to act on messages with "Holiday Cheer" in the Subject line, it will also act on messages whose Subject lines read "Christmas Holiday Cheer" and "Holiday Cheerfulness."

Type	This column only displays data if Sender or Receiver is selected in the **Monitored Field** pick list above. It qualifies the type of sender or receiver whose messages IronMail should monitor. One of three values may be present: • **User:** This indicates that the rule applies to a single email address. An email address (e.g., dscott@mydomain.com) must be provided in the **Data** input field. • **Group:** This indicates that the rule applies to a group of users. If Group is selected, the **Select Group** pick list allows the selection of a group of users. A Mail Monitoring rule may only be applied to a single group of users at a time. If administrators want the rule applied to more than one group, additional rules must be created for each group. Administrators may create groups that contain one or more domains. • **Domain:** This indicates that the rule applies to all members of a single domain. A single *domain name* (e.g., mydomain.com) must be provided in the **Data** input field.
Data	This column displays the specific user, group, or domain whose messages IronMail should monitor. Each Mail Monitoring rule uses the values in the **Monitored Field** and **Type** columns to qualify which messages are to be monitored. Thus, a rule can monitor all messages addressed to a specific domain, or messages from all users of a specified group. The values in this column logically relate to the value in the **Type** column.
Action	When IronMail processes a message matching the criteria specified in the **Monitored Field**, **Type**, and **Data** columns, it can automatically perform an action. One of nine actions may display: • **Secure Delivery:** IronMail will always deliver messages to the specified user, group, or domain securely. First, IronMail will attempt to deliver the message using S/*MIME*. If S/MIME is not supported, IronMail will see if PGP certificates have been installed, and attempt to deliver the message with that method. If IronMail cannot deliver the message with PGP, it will attempt to use *SSL*. If none of these methods are available or supported by the other mail server, IronMail will deliver the message via HTTPS—its Secure Web Delivery. • **Forward as Attachment:** IronMail will create a new message "envelope" and forward the original message as an attachment to an alternate email address. The message still contains the original RFC822 TO address. (The message is forwarded to the address specified in the **Action Value** column.) • **Forward Message:** IronMail will re-write the RFC821 TO address to that displayed in the **Action Value** column. The message is *not delivered* to the original recipient. • **Subject Re-write:** IronMail will prepend an administrator-defined text string to a message's original Subject line. (IronMail prepends the Subject line with the text string appearing in the **Action Value** column.) • **Copy as an attachment:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the **Action Value** column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Copy Message:** IronMail will deliver the original message but send a copy of the message to an alternate address. This action inserts the alternate address in the RFC821 Cc: header—it does not display in the RFC822 Cc: header.

	• **Log:** IronMail will deliver the message to the original recipient, but record in the Mail Monitoring log that a message matching the criteria of the rule was processed. • **Re-route:** IronMail will not deliver the message to the message recipient. Instead, it will deliver the message to another server for additional processing. (The server is identified in the **Action Value** column.) • **Drop Message:** IronMail will drop the message. (Dropped messages are not delivered.) • **Quarantine:** IronMail will send the message to a Quarantine Queue. (When Quarantine is selected, the **Quarantine Type** column will display the specific queue to which the message will be sent.)
Action Value	This column identifies information relevant to the specified Action.
Notify	This column indicates that a notification should be generated if the rule's criteria are met and cause an action to be taken. (Additional notification options are set in *Mail Monitoring > Apply Rules*.)
Delete	To delete a rule from this table, select its **Delete** check box and click **Submit**.

Adding a New Rule

Click **Add New** to create a rule. An Add New Rule window opens. Select options from the available pick lists, and provide related information as required in the user input fields. Click Submit to save the user input. (Click **Close** to close the window without saving the user input.)



Monitored Field	The values in this **Monitored Field** pick list qualify the selection the administrator makes in the Type pick list appearing immediately below. • Select **Sender** to monitor messages originating from a user, group, or domain as specified in the Type pick list below. Messages sent from this or these users will be acted upon accordingly. The Mail Monitoring rule is based on the message's RFC821 FROM address. • Select **Recipient** to monitor messages addressed to a user, group, or domain as specified in the Type pick list below. Messages addressed to this or these users will be acted upon accordingly. The Mail Monitoring rule is based on the message's RFC821 RECIPIENT

	address. • Select **Subject** to monitor messages whose Subject line contains the text string provided in the Data input field below. Note that the search is a sub-string search. If a Mail Monitoring rule is set to act on messages with "Holiday Cheer" in the Subject line, it will also act on messages whose Subject lines read "Christmas Holiday Cheer" and "Holiday Cheerfulness."
Type	The values in this pick list determine the scope of the Mail Monitoring rule. • Select **User** to have IronMail monitor an individual's email. An email address (e.g., dscott@mydomain.com) must be provided in the **Data** input field immediately below. • Select **Group** to have IronMail monitor email for all members of a particular group. If Group is selected, a **Select Group** pick list immediately below allows the selection of a specific group of users. (See Group Manager for information on creating groups.) Note that a Mail Monitoring rule may only be applied to a single group of users. If administrators want the rule applied to more than one group, additional rules must be created for each group. (Note that administrators may create groups that contain one or more domains.) • Select **Domain** to have IronMail monitor email for all members of a domain. A single domain name (e.g., mydomain.com) must be provided in the **Data** input field. (To apply the same rule to multiple domains, create a domain-based group. See Group Manager for information on creating groups.)
Data	Enter in the **Data** input field a value relevant to the User, Group, or Domain value selected from the **Type** pick list above. If User was selected above, an email address is required in this field. If Group was selected above, a secondary **Select Group** pick list is enabled displaying all LDAP or manually generated groups created in Group Manager. If Domain is selecteld, a domain name is required. The **Select Group** pick list also contains a "Global" entry allowing the rule to apply globally to all messages.
Action	Specify the action that should be taken when messages addressed to or sent from specified users, or that contain the specified text string in the Subject line, are received by IronMail. • **Secure Delivery:** IronMail will always deliver *outbound* messages to a specified user, group, or domain securely. (Note that though the Add New Rule interface *appears* to allow the ability to create a Secure Delivery action for inbound mail based on Recipient, Secure Delivery only applies to outbound messages.) First, IronMail will attempt to deliver the message using S/MIME. If S/MIME is not supported, IronMail will attempt to deliver the message using PGP. If neither is supported by the other mail server, IronMail will attempt to deliver the message with SSL. If SSL is unsupported, IronMail will fall back to Secure Web Delivery. (If a Secure Web Delivery user account has already been created for the recipient, IronMail will not attempt to use SSL.) • **Forward as Attachment:** IronMail will create a new email with the original message included as a file attachment. When "forwarded as an attachment," the original email will not display in the email client's Preview window—a useful option, for example, if the rule is designed to detect pornographic messages. When this action is selected, the message is not delivered to the original recipient. The message is forwarded to the address specified in the Action Value column.

	• **Forward Message:** IronMail will re-write the RFC821 TO address and forward the message to the address specified in the Action Value column. • **Subject Rewrite:** IronMail will prepend a text string to the beginning of a message's original Subject line. (IronMail prepends the Subject line with the text string provided in the Action Value field below.) • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Log:** IronMail will deliver the message to the original recipient, but record in the Mail Monitoring Policy Compliance Report that a message matching the criteria of the rule was processed. • **Re-route:** IronMail will not deliver the message to the recipient, but instead deliver it to another server for additional processing. (The server must be identified in the Action Value input field below.) • **Drop Message:** IronMail will drop the message. (Dropped messages are not delivered.) • **Quarantine:** IronMail will send the message to a quarantine queue.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** pick list will be enabled, and display all queues that have been created in *Queue Manager > Quarantine Types*. Select the specific queue the rule should send messages to.
Action Value	Some actions require specific data, or values, to be provided in order for IronMail to complete the operation. • **Secure Delivery** does not require an Action Value. • **Forward as Attachment** requires a valid email address. Multiple addresses may be entered, but they must be separated by a comma delimiter. • **Forward Message** requires a valid email address. Multiple addresses may be entered, but they must be separated by a comma delimiter. • **Subject Re-write** requires a text string. The string may be of any length and may contain any printable character the keyboard can produce—with one exception: the "pipe" symbol ("|") may not be used. • **Copy Message** requires a valid email address. Multiple addresses may be entered, but they must be separated by a comma delimiter. • **Log** does not require a value in the **Action Data** field. • **Re-route** requires either an *IP address* or fully qualified *host name* (e.g., "192.168.16.5" or "hostname.domain.com). • **Drop Message** does not require an Action Value. • **Quarantine** requires a numeric value between 0 and 15. The number refers to how many days the message sits in a quarantine queue before IronMail releases it to any remaining queues that have yet to process the message. For example, if the message enters IronMail at 2 PM on Wednesday, and the Quarantine value is "2," IronMail will automatically release the message for delivery at ~2:01 PM Friday. A "0" in this field signifies "do not deliver." The message will sit in the quarantine queue until IronMail's Cleanup subsystem deletes quarantined data as specified by the Cleanup Schedule (see *System > Cleanup Schedule*).

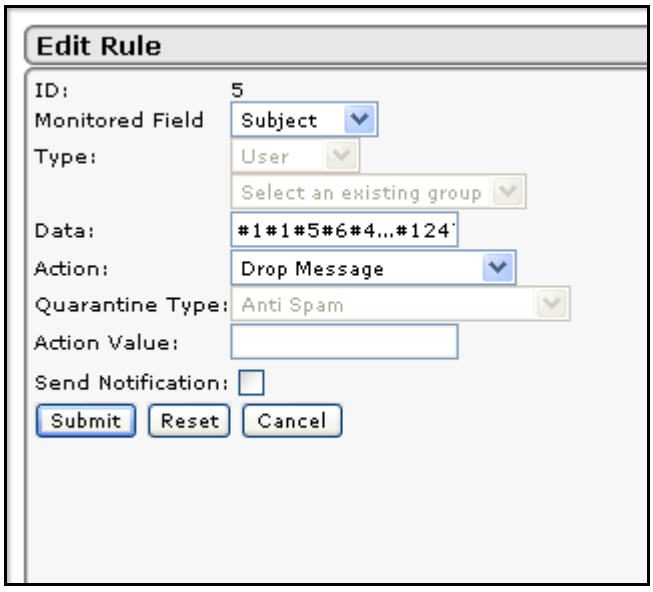
Send Notification	Select the **Send Notification** check box to have IronMail generate a notification that an action was taken on a message because of the rule. The notification goes to the message's sender outside the *network* or either the sender or receiver if inside the network, as specified in *Policy Manager > Mail Monitoring > Apply Rules*. "Notifications" may be customized at *Policy Manager > Notification*.

Click **Submit** in the secondary browser to save the user input, or **Close** to close the window without saving user input. If **Submit** is clicked and required fields are empty, or fields contain invalid information, an alert message will report which field contains invalid data.

Mail Monitoring rules are not active until they are applied to users or groups of users. Turn a Mail Monitoring rule into an active "policy" by navigating to *Policy Manager > Mail Monitoring > Apply Rules* and apply the rule to users.

Editing an Existing Rule

Clicking on the ID hyperlink in the Mail Monitoring Rule Management screen opens an Edit Rule window where the specific rule can be modified.



Change the information on the screen as necessary.

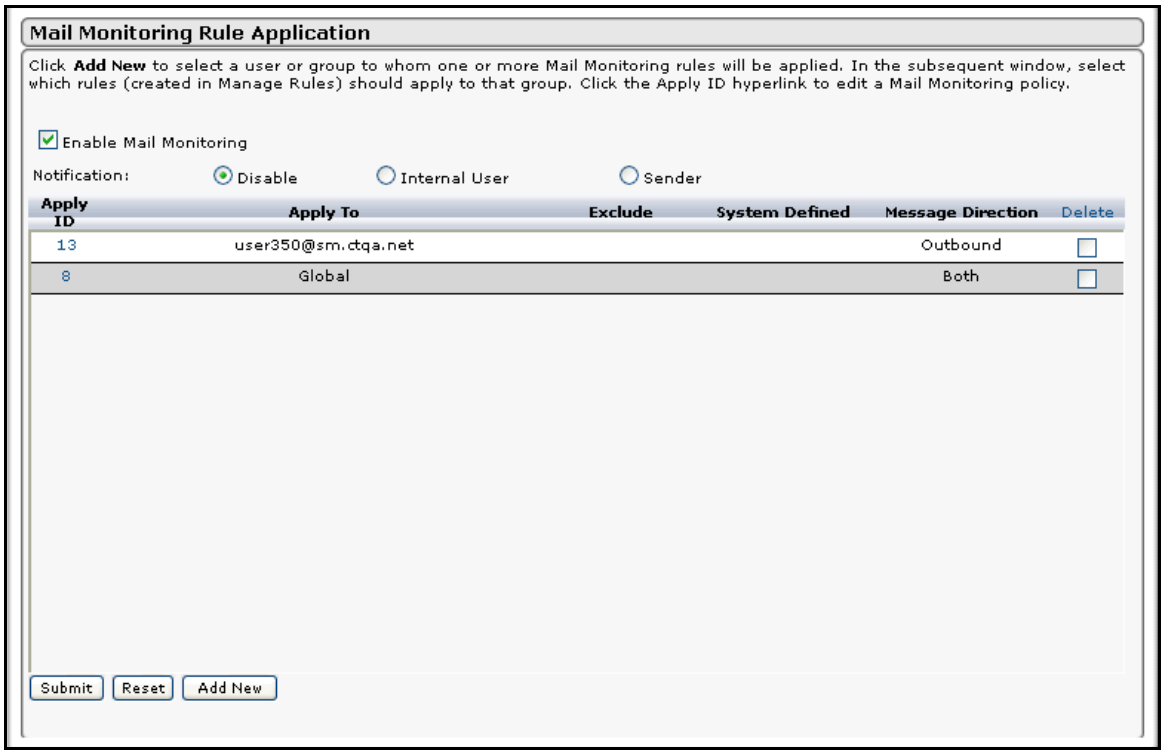
Field	Description
ID	The ID is system-determined and assigned to the rule when it is created. The ID is not editable.
Monitored Field	Select Sender, Recipient or Subject from the pick list.
Type	To change the type of entity to be monitored by the rule, select User, Group or Domain from the pick list.
Data	Enter the email address for the user, or the domain name for a domain rule. For a group rule, select an existing group from the drop-down list.
Action	Select the action to be taken when messages to or from specified users, or with subject lines containing specified text strings, are detected.

Quarantine Type	If Quarantine is the selected action, choose the quarantine type from the pick list.
Action Value	Enter the appropriate data to define the selected action, such as the number of days for quarantine, the address to which mail should be forwarded, etc.
Send Notification	Checking this box enables IronMail to send notices as configured when a policy built on this rule is triggered.

Click Submit to enter your changes. The Mail Monitoring Rule Management screen will be refreshed.

Apply Rules

Mail Monitoring *rules* are created in *Policy Manager* > *Mail Monitoring* > *Manage Rules*, but they do not become active until they are applied to specific users or groups. Only after the rules are converted into Mail Monitoring *policies* in this window will IronMail take the specified actions for messages IronMail processes.



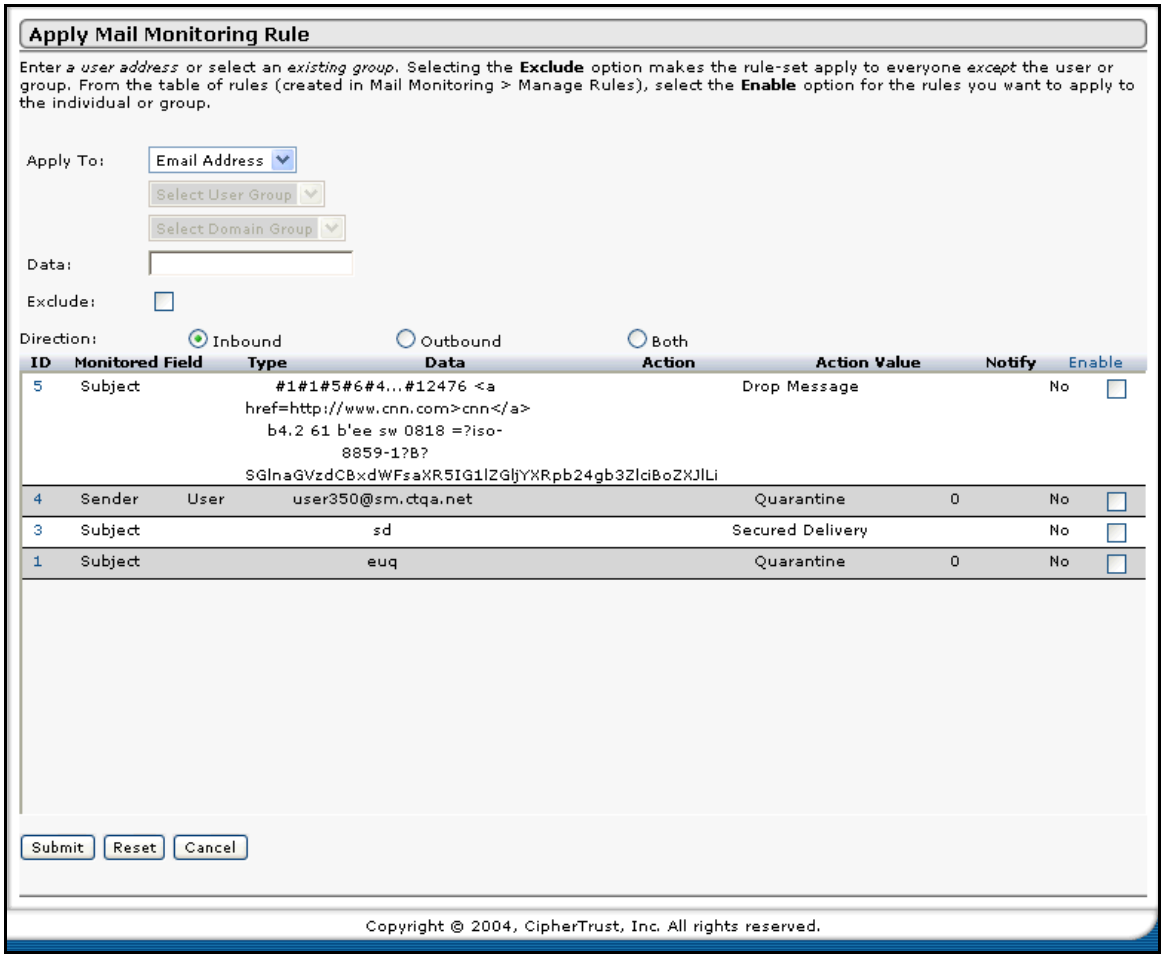
The screen provides the following information:

Enable Mail Monitoring	Select the **Enable Mail Monitoring** check box to enable, or "turn on," Mail Monitoring. If enabled, IronMail will examine the Subject line, or Sender or Receiver information, of every message it receives, and check if the data in those fields match the values contained in any active Mail Monitoring *rule*. Note that Mail Monitoring policies are enforced, or processed, in the Mail Monitoring Queue, one of IronMail's queue subsystems. Therefore, the Mail Monitoring Queue must be set to Auto-Start, Running, and assigned a "queue position." The Web Administration user interface will allow "Enable Mail Monitoring" to be selected even if the Mail Monitoring Queue is not currently running, but the Mail Monitoring policies will not be enforced until the queue is enabled.

Notification	When Mail Monitoring rules were created in the *Policy Manager > Mail Monitoring > Manage Rules* page, an option provided for a notification to be generated if the rule acted upon a message. The notification setting here relates to that option. Three qualifying choices are available: • Select **Disable** to override the notification setting within individual Mail Monitoring rules. If this radio button is selected, IronMail will not generate any notifications if Mail Monitoring rules affect a message. • Select **Internal User** to send notifications only to users inside the *network*. Regardless of whether the internal user is the recipient or sender of the message, IronMail will generate a notification to him or her if a Mail Monitoring policy took an action on the message. • Select **Sender** to send notifications only to the message sender—the individual identified in the email's FROM address—regardless whether or not the sender is inside or outside the network.
Policies	***The lower part of the screen, empty until policies are created, is a table of policies.***
Apply ID	IronMail identifies each policy that will be processed by the Mail Monitoring Queue with a unique, serially incrementing ID number. (Therefore the ID numbers for Encrypted Message Filtering, Mail Monitoring, and Message Stamping policies will not be duplicated—each time a policy within any of those three program areas is created, it is assigned the next higher number.) IronMail's logs and Daily Policy Compliance Reports will report the policy ID number when messages match the criteria of specific policies. The ID number is also a hyperlink that opens a secondary browser window in which the policy may be edited.
Apply To	This column reports the individual or group to whom the specific policy applies.
Exclude	A mark in the **Exclude** column indicates that the policy applies globally to everyone except the specified individual or group.
System Defined	A mark in this column indicates that the policy was generated by another IronMail process. For example, End User Spam Reporting and the Anomaly Detection Engine are both capable of creating Mail Monitoring rules. Note that "system-generated" policies cannot be deleted within this table of Mail Monitoring policies. That is, the **Delete** check box is disabled for system-generated policies. On the other hand, the policy may be edited within the secondary Edit window if the policy ID number hyperlink is clicked. If all the rules of a system-generated policy are deleted from the secondary Edit window, the policy is deleted and removed from the table.
Message Direction	This column indicates the "direction" of mail for which the policy applies. One of three values will display: • **Inbound:** the policy only affects incoming messages addressed to the specified user or group. • **Outbound:** the policy only affects outgoing messages originating from the specified user or group. • **Both:** the policy affects all messages to or from the specified user or group.
Delete	To delete a policy, select its **Delete** check box and click **Submit**. Note that "system-generated" policies cannot be deleted within this table of Mail Monitoring policies. That is, the **Delete** check box is disabled for system-generated policies. On the other hand, the policy may be edited within the secondary Edit window if the policy ID number hyperlink is clicked. If all the rules of a system-generated policy are deleted from the secondary Edit window, the policy is deleted and removed from the table.

Adding a New Policy

Click **Add New** to generate a new policy based on specific rules created in *Policy Manager > Mail Monitoring > Manage Rules*. An Apply Mail Monitoring Rule secondary browser window opens.



Provide the following input:

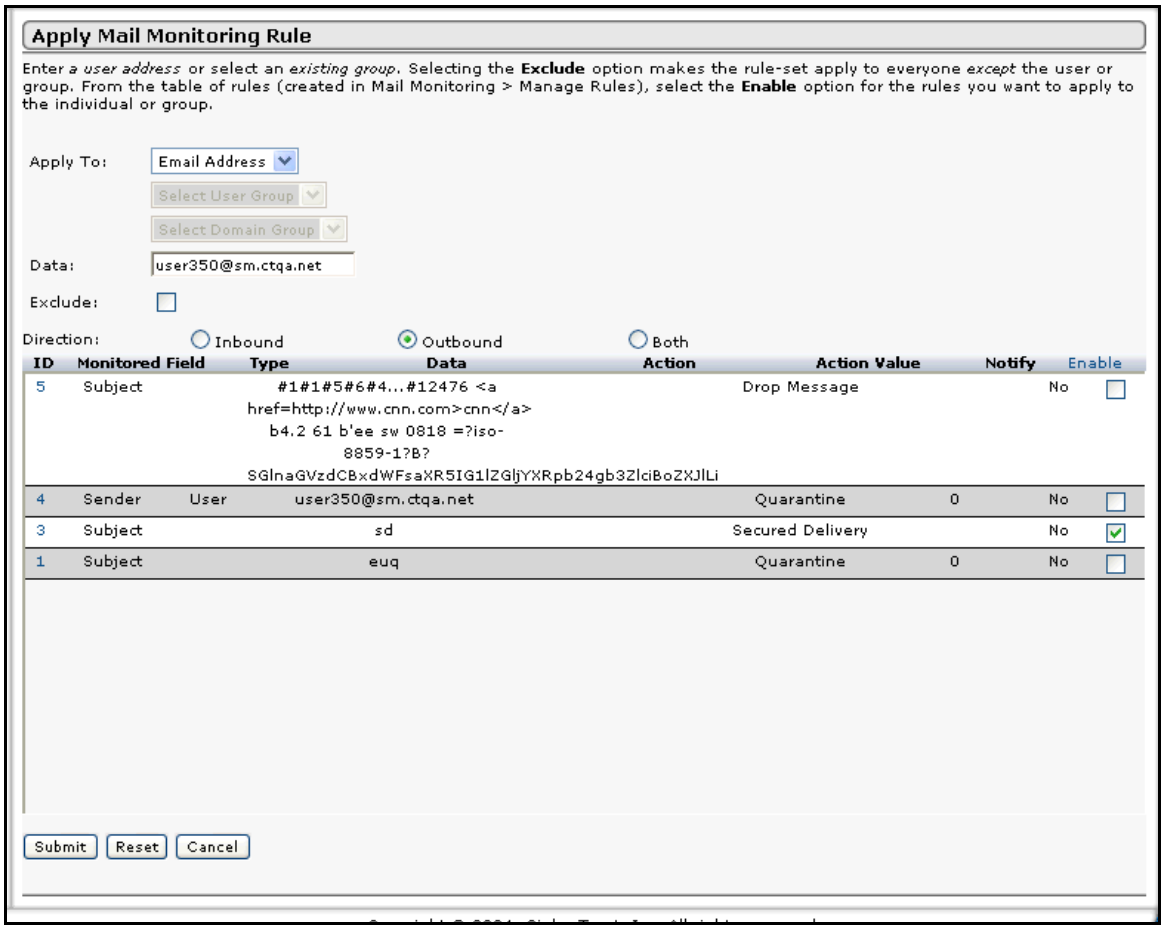
Apply To	Select the type of entity to which the policy will apply. Options are: • User • Group • Domain
Data	If the policy is to be applied to an email address, enter that address in the data field. Otherwise, select the proper group or domain information from the drop down lists. Multiple email addresses are not allowed in the User field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required. Also, a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. A selection of "Global" applies the policy to all users.

Exclude	Select the **Exclude** check box to apply the policy to everyone *except* the specified user or group. For example, if a rule states that messages originating from Yahoo.com are to be quarantined, and this policy is applied to Management exclusively, then the only users whose mail from Yahoo.com will not be quarantined are members of the Management group.
Direction	Specify the direction of mail for which the policy applies. • **Inbound Messages:** the policy only affects incoming messages addressed to the specified user or group. • **Outbound Messages:** the policy only affects outgoing messages originating from the specified user or group. • **Both:** the policy affects all messages to or from the specified user or group.
Table of Rules	***Below the three input fields is a table displaying all Mail Monitoring rules that have been created. Each row in the table corresponds to a specific rule.***
ID	The column shows the ID number for each rule that has been created. The ID number is also a hyperlink for editing the rule.
Monitored Field	This column indicates the field the rule is monitoring: Sender, Recipient, or Subject.
Type	The column indicates the type of entity to which the rule will apply. Options are: • User • Group • Domain
Data	Any data associated with the monitored field shows in this column.
Action	The action associated with the rule is listed here.
Action Value	This column shows any action information (e.g., quarantine type, etc.) associated with the action.
Notify	If this rule results in notifications being sent, that will be indicated in this column.
Enable	The Enable checkbox determines if the rule is in use by the policy or not. The Enable hyperlink toggles all rules on and off.

Click **Submit** to save the user input and create the policy. (The policy now displays in the Mail Monitoring Rule Application table in the Web Administration interface.) Click **Add New** again to create additional policies.

Editing an Existing Policy

Clicking the Apply ID link on the Mail Monitoring Rule Application screen opens a screen that looks like the version of that screen used for adding rules. The difference is that this screen is already populated with the information about the existing policy. To edit the policy, you simply change the information.



Apply To	Select the type of entity to which the policy will apply. Options are: • User • Group • Domain
Data	If the policy is to be applied to an email address, enter that address in the data field. Otherwise, select the proper group or domain information from the drop down lists. Multiple email addresses are not allowed in the User field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required. Also, a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. A selection of "Global" applies the policy to all users.
Exclude	Select the **Exclude** check box to apply the policy to everyone *except* the specified user or group. For example, if a rule states that messages originating from Yahoo.com are to be quarantined, and this policy is applied to Management exclusively, then the only users whose mail from Yahoo.com will not be quarantined are members of the Management group.

Direction	Specify the direction of mail for which the policy applies. • **Inbound Messages:** the policy only affects incoming messages addressed to the specified user or group. • **Outbound Messages:** the policy only affects outgoing messages originating from the specified user or group. • **Both:** the policy affects all messages to or from the specified user or group.
Table of Rules	***Below the three input fields is a table displaying all Mail Monitoring rules that have been created. Each row in the table corresponds to a specific rule.***
ID	The column shows the ID number for each rule that has been created. The ID number is also a hyperlink for editing the rule.
Monitored Field	This column indicates the field the rule is monitoring: Sender, Recipient, or Subject.
Type	The column indicates the type of entity to which the rule will apply. Options are: • User • Group • Domain
Data	Any data associated with the monitored field shows in this column.
Action	The action associated with the rule is listed here.
Action Value	This column shows any action information (e.g., quarantine type, etc.) associated with the action.
Notify	If this rule results in notifications being sent, that will be indicated in this column.
Enable	The Enable checkbox determines if the rule is in use by the policy or not. The Enable hyperlink toggles all rules on and off.

Mail Monitoring Order of Precedence

There may be occasions when a single message is "flagged for action" by more than one Mail Monitoring policy. For example, one policy might state that messages originating from *spamdomain.com* are to be deleted, and another policy might state that mail addressed to *individual@domain.com* is to be quarantined. If a message is addressed to *individual@domain.com* and originates from *spamdomain.com*, two conflicting actions are required. Therefore, IronMail follows an order of precedence in which the policies' actions take place, as stated in the following three paragraphs:

The first test of precedence is whether the policy contains **System**- or **User-generated** rules. Policies containing **System-generated** rules act on messages before policies containing User-generated rules.

The second test of precedence is whether the policy applies to an **individual** or a **member of a group**. Policies applied to **individuals** take precedence to policies applied to **members of a group**.

The final test of precedence is based on the policy's action. The **Re-route** action takes first precedence, followed by **drop**, followed by **quarantine**, followed by **forward**, followed by **copy**, **subject re-write**, and **log**. (**Subject re-write**, **copy** and **log** share precedence because neither precludes the implementation of the others.)

Encrypted Messages

Encrypted Message Filtering

While client-based encryption and digital signatures are a valuable addition to email security, guaranteeing that mail really came from the stated sender and was not altered in transit, it can also protect viruses, malicious code, and the actions of unscrupulous employees. Once encrypted on the client side, a message cannot be examined by IronMail. Administrators, therefore, don't know if an encrypted message is giving away company secrets, contains offensive material, or is carrying destructive code. Note that IronMail is capable of detecting S/*MIME* Version 2 (RFC2311), Open PGP (RFC2440), and MIME Security for PGP (RFC3156) encryption.

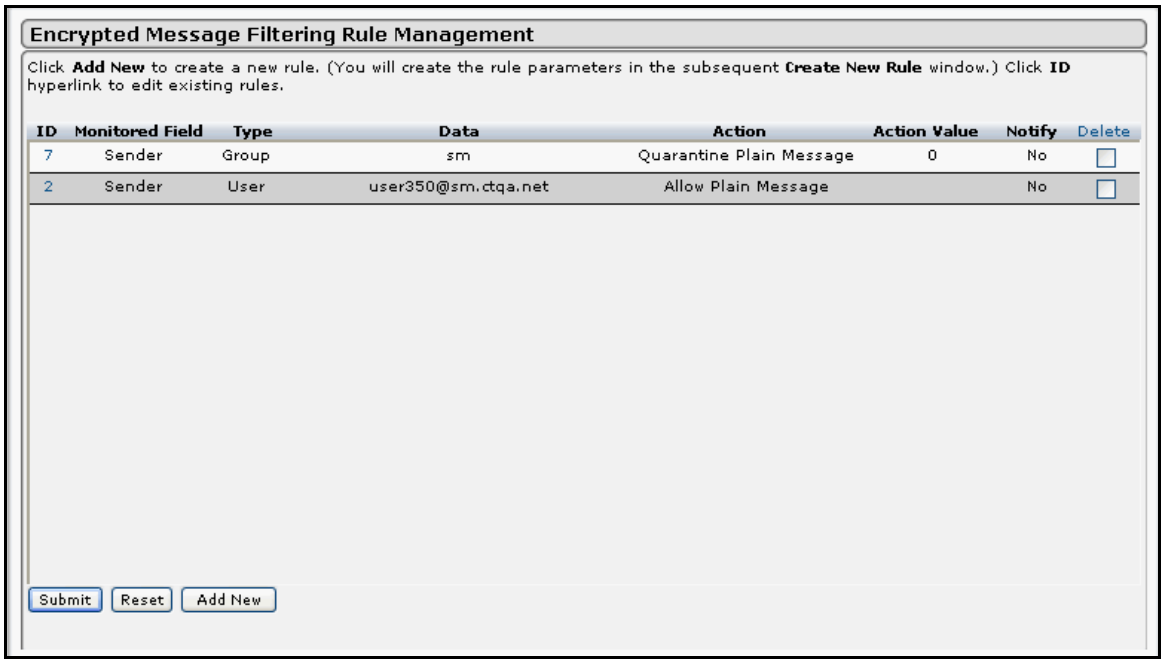
IronMail provides the ability to create and enforce policies specifying who may send and receive digitally signed and client-encrypted email. Encrypted Message Filtering rules may be applied to individual users, to groups, and to domains. Policies applied to users take precedence over policies applied to groups and domains. In this program area, all configuration settings apply both to the use of digital signatures as well as encrypted messaging.

Encrypted Message Filtering policies are processed in IronMail's Mail Monitoring process. That is, when messages enter the IronMail appliance, each of IronMail's features compares the message characteristics with the specific rules outlined in the related *policy*. Accordingly, Mail Monitoring must be running in order for Encrypted Message Filtering policies to be enforced.

The Encrypted Message Filtering hyperlink in the left navigation frame expands to offer Manage Rules and Apply Rules sub-menus.

Manage Rules

Encrypted Message Filtering *rules* are created, edited, and deleted in the Encrypted Message Filtering *Rule* Management program area. (The rules do not become "active" until they are applied to specific users or groups, at which point the rules become *policies*.)


Encrypted Message Filtering Rule Management
Click Add New to create a new rule. (You will create the rule parameters in the subsequent Create New Rule window.) Click ID hyperlink to edit existing rules.
ID Monitored Field Type Data Action Action Value Notify Delete
7 Sender Group sm Quarantine Plain Message 0 No
2 Sender User user350@sm.ctqa.net Allow Plain Message No
Submit
Reset
Add New

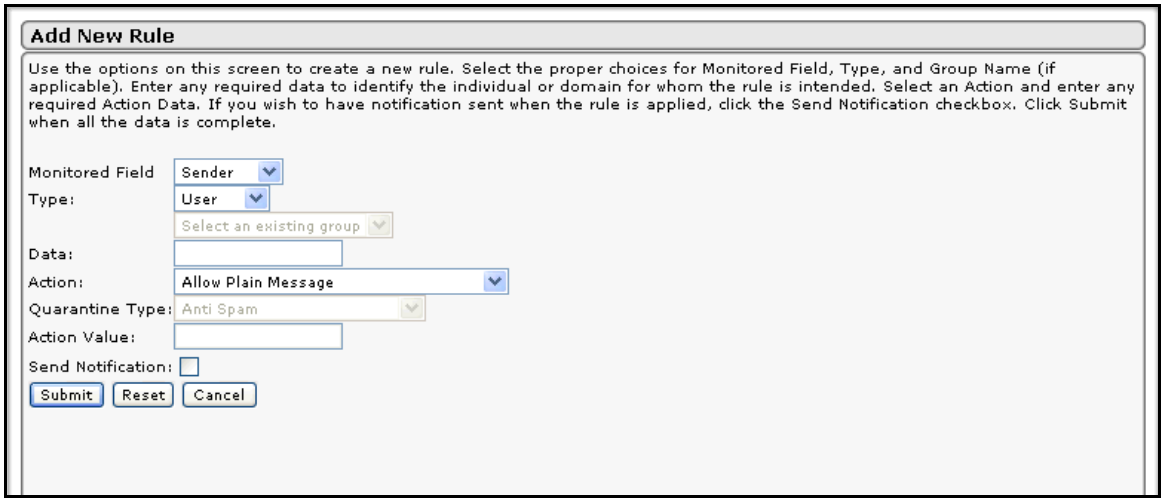
The Encrypted Message Filtering Rule Management table, empty until rules have been created, displays information about the individual rules.

Field	Description

ID	This column displays the unique ID number that IronMail generates for each Encrypted Message Filtering rule. Whenever a *policy* is enforced, IronMail's reports or logs will provide information about the message, and the specific Encrypted Message Filtering Rule ID responsible for causing IronMail to act on the message. Rule ID numbers are serially incremented. If a rule is deleted, IronMail does not re-use its ID number. The Rule ID is also a hyperlink opening a window in which the rule may be edited.
Monitored Field	This column identifies the field in the message to be monitored by this rule. Options are: • Sender • Recipient • Subject
Type	This column indicates if the rule will affect messages for a user, group or domain.
Data	This column identifies the user, group, or domain whose messages will be affected by the Encrypted Message Filtering rule. If the rule is based on an individual, an email address will display. If the rule is based on a group, the name of the group will be displayed.
Action	The rule's action is identified. One of six values will display: • Drop encrypted message • Drop plain message • Quarantine encrypted message • Quarantine plain message • Allow encrypted message • Allow plain message
Action Value	This column will display qualifying information related to the rule's action. Only a quarantine action requires qualifying information—a specified number of days the message is to be quarantined.
Notify	This column indicates that notification has been enabled. If the Encrypted Message Filtering rule takes an action on a message, a notification can be delivered. Notifications may be customized at *Policy Manager > Notification*. Note that administrators configure who will receive notifications in *Policy Manager > Encrypted Message Filtering > Apply Rules*.
Delete	Select a rule's **Delete** check box and click **Submit** to delete a rule. The **Delete** column heading is also a hyperlink. Clicking **Delete** selects all the rules in the Encrypted Message Filtering Rule Management table. (Clicking **Delete** a second time de-selects all the rules.)

Adding a New Rule

Click **Add New** to create a new Encrypted Message Filtering rule. The Add New Rule screen opens.


Add New Rule
Use the options on this screen to create a new rule. Select the proper choices for Monitored Field, Type, and Group Name (if applicable). Enter any required data to identify the individual or domain for whom the rule is intended. Select an Action and enter any required Action Data. If you wish to have notification sent when the rule is applied, click the Send Notification checkbox. Click Submit when all the data is complete.
Monitored Field
Sender
Type:
User
Select an existing group
Data:
Action:
Allow Plain Message
Quarantine Type:
Anti Spam
Action Value:
Send Notification:
Submit
Reset
Cancel

The window requests the following user input:

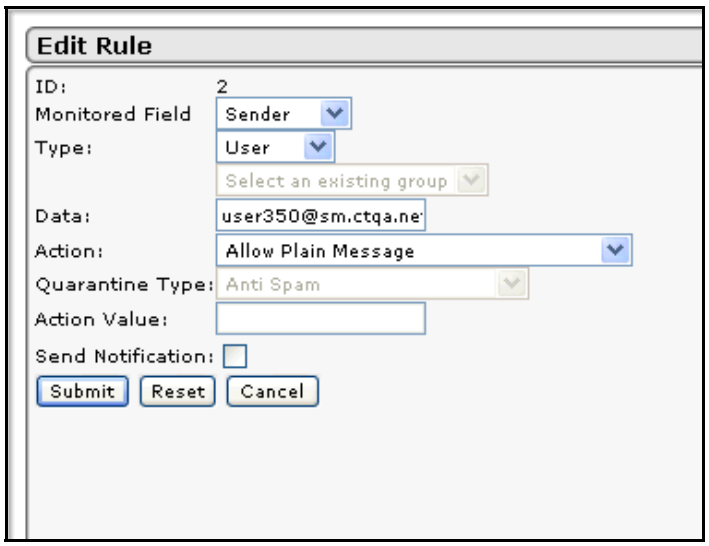
Field	Description
Monitored Field	The values in this **Monitored Field** pick list qualify the selection the administrator makes in the **Type** pick list below. • Select **Sender** to monitor messages originating from a user, group, or domain as specified in the **Type** pick list below. Messages sent from this or these users will be acted upon accordingly. The Encrypted Message Filtering rule is based on the message's RFC821 FROM address. • Select **Recipient** to monitor messages addressed to a user, group, or domain as specified in the **Type** pick list below. Messages addressed to this or these users will be acted upon accordingly. The Encrypted Message Filtering rule is based on the message's RFC821 RECIPIENT address.
Type	The values in this pick list determine the scope of the Encrypted Message Filtering rule. • Select **User** to have IronMail monitor an individual's email. An email address (e.g., dscott@mydomain.com) must be provided in the Data input field immediately below. • Select **Group** to have IronMail monitor email for all members of a particular group. If **Group** is selected, a **Select Group** pick list immediately below allows the selection of a specific group of users. (See Group Manager for information on creating groups.) An Encrypted Message Filtering rule may only be applied to a single group of users. If administrators want the rule applied to more than one group, additional rules must be created for each group. Administrators may create groups that contain one or more domains. • Select **Domain** to have IronMail monitor email for all members of a domain. A single domain name (e.g., mydomain.com) must be provided in the **Data** input field. To apply the same rule to multiple domains, create a domain-based group. See Group Manager for information on creating groups.

Data	If "User" or "Domain" is selected in the **Type** pick list above, the specific email address or *domain name* must be provided. (If "Group" was selected, the name of the group is automatically inserted in the **Data** input field.)
Action	Select an action IronMail should take for messages addressed to or received from specified users: • **Drop encrypted message:** if the message is encrypted, IronMail will drop it, i.e. encrypted messaging *is not allowed*. • **Drop plain message:** if the message is not encrypted, drop it, i.e. encrypted messaging is *required*. • **Quarantine encrypted message:** if the message is encrypted, send it to a quarantine queue. This action allows administrative review of encrypted messages. When selected, a numeric value must be provided in the **Action Value** input field below, representing how many days the message will be quarantined. If this option is enabled, a **Quarantine Type** pick list is enabled, displaying all system- or manually-created quarantine queues. A quarantine queue must be specified. • **Quarantine plain message:** if the message is not encrypted, send it to a quarantine queue. This action allows administrative review of unencrypted messages. When selected, a numeric value must be provided in the **Action Value** input field below, representing how many days the message will be quarantined. • **Allow encrypted message:** encrypted messaging is allowed, i.e. users for whom the policy applies are allowed to send encrypted messages. • **Allow plain message:** plain text messaging is allowed, i.e. users for whom the policy applies are not required to send encrypted messages.
Quarantine Type	If the quarantine option is enabled, a **Quarantine Type** pick list is also enabled, displaying all system- or manually-created quarantine queues. A quarantine queue must be specified.
Action Value	The **Action Value** input field is only active if a quarantine action is selected in the **Action** pick list. A number, from 0 to 15 must be entered, representing the number of days before IronMail automatically delivers the message to the original recipient. For example, if a value of "2" is entered, a message entering a quarantine queue at 3 PM on Wednesday will be delivered at approximately 3:01 PM on Friday. Note that a zero value ("0") represents "do not deliver." IronMail's Cleanup subsystem will automatically delete messages that have sat in a quarantine queue longer than specified in the Cleanup Schedule (*System > Cleanup Schedule > "Quarantine Data"*). If a zero is entered in this field, messages will not be delivered unless the administrator manually creates a "delivery time" for them. See *Queue Manager > Quarantine Queue > secondary Message Headers* window for information on moving messages out of a quarantine queue.
Send Notification	Select the **Send Notification** check box to have IronMail generate a notification that an action was taken on a message because of the rule. The notification goes to the message's sender outside the *network* or either the sender or receiver if inside the network. Additional notification parameters are configured in *Policy Manager > Mail Monitoring > Apply Rules*. Notifications may be customized at *Policy Manager > Notification*.

When the information has been entered correctly, click **Submit** to create the new rule.

Editing an Existing Rule

Clicking the ID hyperlink on the Encrypted Message Filtering Rule Management screen opens the Edit Rule screen below. The content of this screen is identical to the fields on the Add New Rule, screen, with the exceptions that the rule's ID number is included at the top of the screen, and the fields are pre-populated with existing configuration information.



To edit the rule, make changes to the information on the screen.

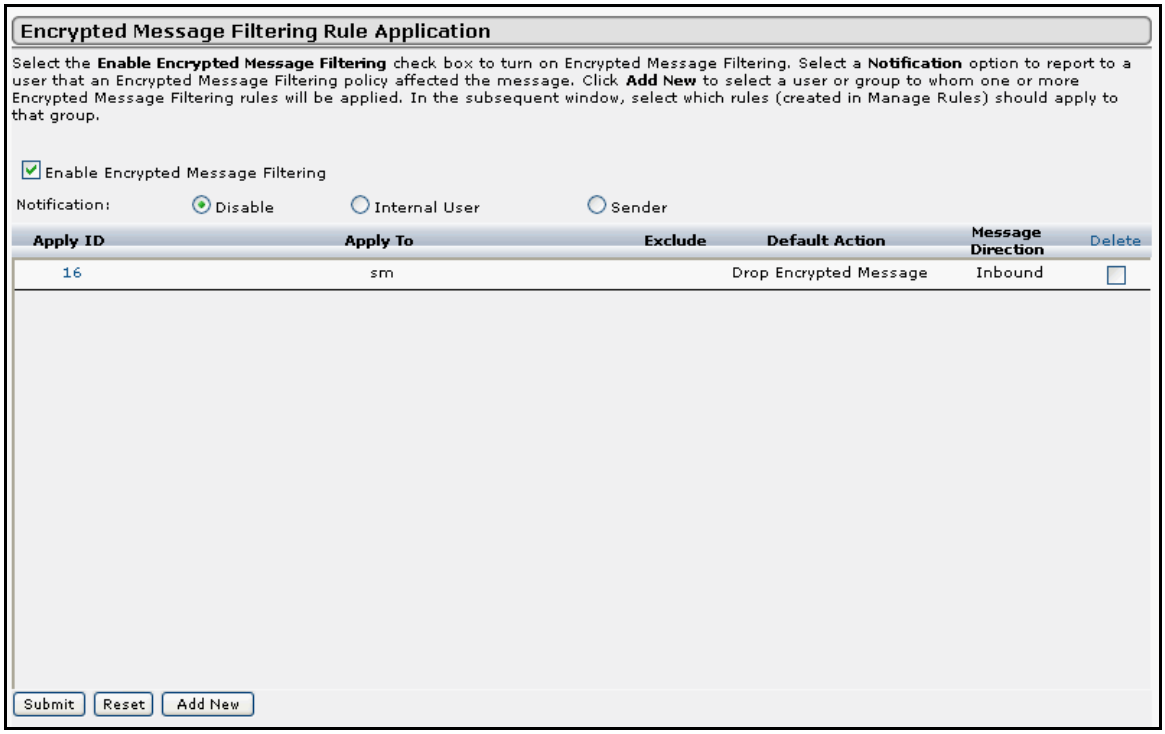
Field	Description
Monitored Field	The values in this **Monitored Field** pick list qualify the selection the administrator makes in the **Type** pick list below. • Select **Sender** to monitor messages originating from a user, group, or domain as specified in the **Type** pick list below. Messages sent from this or these users will be acted upon accordingly. The Encrypted Message Filtering rule is based on the message's RFC821 FROM address. • Select **Recipient** to monitor messages addressed to a user, group, or domain as specified in the **Type** pick list below. Messages addressed to this or these users will be acted upon accordingly. The Encrypted Message Filtering rule is based on the message's RFC821 RECIPIENT address.
Type	The values in this pick list determine the scope of the Encrypted Message Filtering rule. • Select **User** to have IronMail monitor an individual's email. An email address (e.g., dscott@mydomain.com) must be provided in the Data input field immediately below. • Select **Group** to have IronMail monitor email for all members of a particular group. If **Group** is selected, a **Select Group** pick list immediately below allows the selection of a specific group of users. (See Group Manager for information on creating groups.) An Encrypted Message Filtering rule may only be applied to a single group of users. If administrators want the rule applied to more than one group, additional rules must be created for each group. Administrators may create groups that contain one or more domains. • Select **Domain** to have IronMail monitor email for all members of a domain. A single domain name (e.g., mydomain.com) must be

	provided in the **Data** input field. To apply the same rule to multiple domains, create a domain-based group. See Group Manager for information on creating groups.
Data	If "User" or "Domain" is selected in the **Type** pick list above, the specific email address or domain name must be provided. (If "Group" was selected, the name of the group is automatically inserted in the **Data** input field.)
Action	Select an action IronMail should take for messages addressed to or received from specified users: • **Drop encrypted message:** if the message is encrypted, IronMail will drop it, i.e. encrypted messaging *is not allowed*. • **Drop plain message:** if the message is not encrypted, drop it, i.e. encrypted messaging is *required*. • **Quarantine encrypted message:** if the message is encrypted, send it to a quarantine queue. This action allows administrative review of encrypted messages. When selected, a numeric value must be provided in the **Action Value** input field below, representing how many days the message will be quarantined. If this option is enabled, a **Quarantine Type** pick list is enabled, displaying all system- or manually-created quarantine queues. A quarantine queue must be specified. • **Quarantine plain message:** if the message is not encrypted, send it to a quarantine queue. This action allows administrative review of unencrypted messages. When selected, a numeric value must be provided in the **Action Value** input field below, representing how many days the message will be quarantined. • **Allow encrypted message:** encrypted messaging is allowed, i.e. users for whom the policy applies are allowed to send encrypted messages. • **Allow plain message:** plain text messaging is allowed, i.e. users for whom the policy applies are not required to send encrypted messages.
Quarantine Type	If the quarantine option is enabled, a **Quarantine Type** pick list is also enabled, displaying all system- or manually-created quarantine queues. A quarantine queue must be specified.
Action Value	The **Action Value** input field is only active if a quarantine action is selected in the **Action** pick list. A number, from 0 to 15 must be entered, representing the number of days before IronMail automatically delivers the message to the original recipient. For example, if a value of "2" is entered, a message entering a quarantine queue at 3 PM on Wednesday will be delivered at approximately 3:01 PM on Friday. Note that a zero value ("0") represents "do not deliver." IronMail's Cleanup subsystem will automatically delete messages that have sat in a quarantine queue longer than specified in the Cleanup Schedule (*System > Cleanup Schedule > "Quarantine Data"*). If a zero is entered in this field, messages will not be delivered unless the administrator manually creates a "delivery time" for them. See *Queue Manager > Quarantine Queue > secondary Message Headers* window for information on moving messages out of a quarantine queue.
Send Notification	Select the **Send Notification** check box to have IronMail generate a notification that an action was taken on a message because of the rule. The notification goes to the message's sender outside the network or either the sender or receiver if inside the network. Additional notification parameters are configured in *Policy Manager > Mail Monitoring > Apply Rules*. Notifications may be customized at *Policy Manager > Notification*.

Click **Submit** to save the user input and create the rule. Click **Close** to close the Edit Rule window. (Clicking **Close** before clicking **Submit** causes the loss of any user input.)

Apply Rules

Encrypted Message Filtering *rules* are created in *Policy Manager > Encrypted Message Filtering > Manage Rules*, but they do not become active until they are applied to specific users or groups. Only after the rules are converted into Encrypted Message Filtering *policies* in this window will IronMail take the specified actions for messages it processes.

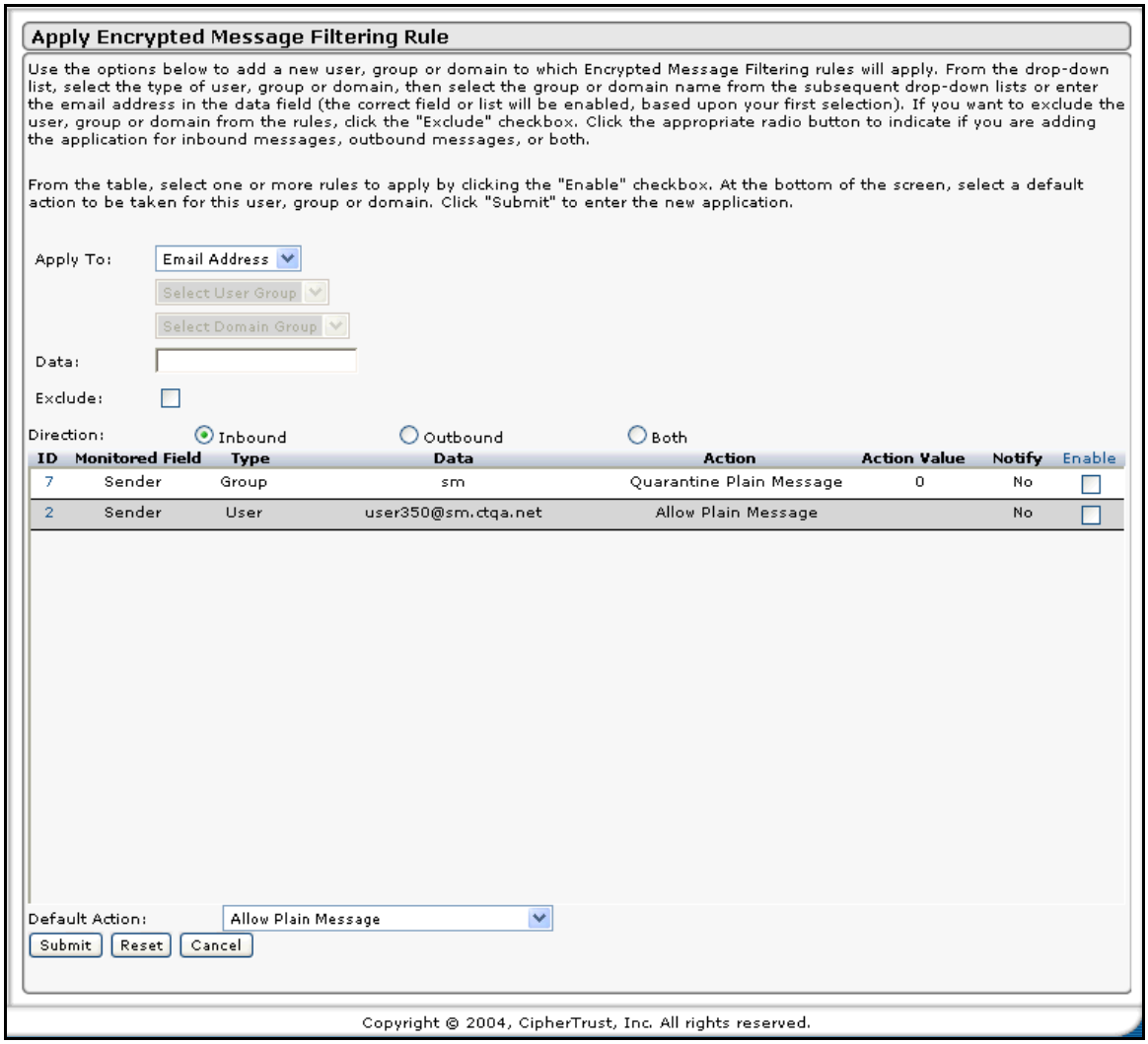

Encrypted Message Filtering Rule Application
Select the Enable Encrypted Message Filtering check box to turn on Encrypted Message Filtering. Select a Notification option to report to a user that an Encrypted Message Filtering policy affected the message. Click Add New to select a user or group to whom one or more Encrypted Message Filtering rules will be applied. In the subsequent window, select which rules (created in Manage Rules) should apply to that group.
Enable Encrypted Message Filtering
Notification:
Disable
Internal User
Sender
Apply ID
Apply To
Exclude
Default Action
Message Direction
Delete
16
sm
Drop Encrypted Message
Inbound
Submit
Reset
Add New

Field	Description
Enable Encrypted Message Filtering	Select the **Enable Encrypted Message Filtering** check box to enable, or "turn on," Encrypted Message Filtering. If enabled, IronMail will enforce the Encrypted Message Filtering policies listed in the table below. Note that Encrypted Message Filtering policies are enforced, or processed, in the Mail Monitoring Queue, one of IronMail's queue subsystems. Therefore, the Mail Monitoring Queue must be set to Auto-Start, Running, and assigned a "queue position." The Web Administration user interface will allow **Enable Encrypted Message Filtering** to be selected even if the Mail Monitoring Queue is not currently running, but the Encrypted Message Filtering policies will not be enforced until the queue is enabled.

Notification	When Encrypted Message Filtering rules were created in the *Policy Manager > Encrypted Message Filtering > Manage Rules* page, an option provided for a notification to be generated if the *rule* acted upon a message. The notification setting here relates to that option. Three qualifying choices are available: • Select **Disable** to override the notification setting within individual Encrypted Message Filtering rules. If this radio button is selected, IronMail will not generate any notifications if Encrypted Message Filtering rules affect a message. • Select **Internal User** to send notifications only to users inside the *network*. Regardless of whether the internal user is the recipient or sender of the message, IronMail will generate a notification to him or her if an Encrypted Message Filtering policy took an action on the message. • Select **Sender** to send notifications to the message sender—regardless of whether he or she is inside or outside of the network.
Table of Policies	***The lower portion of the screen is a table showing all currently existing policies.***
Apply ID	IronMail identifies each policy with a unique, serially incrementing ID number. Note that IronMail's serial numbers span all policies processed by the Mail Monitoring Queue. Thus, the ID numbers for Encrypted Message Filtering, Mail Monitoring, and Message Stamping policies will not be duplicated—each time a policy within any of those three program areas is created, it is assigned the next higher number. IronMail's logs and Daily Policy Compliance Reports will report the policy ID number when messages meet the criteria of specific policies. The ID number is also a hyperlink that opens a secondary browser window in which the policy may be edited.
Apply To	This column reports the individual or group to whom the specific policy applies.
Exclude	A mark in the **Exclude** column indicates that the policy applies globally to everyone *except* the specified individual or group.
Default Action	The default action associated with the specific rule displays in this column.
Message Direction	This column indicates the "direction" of mail for which the policy applies. One of three values will display: • **Inbound:** the policy only affects incoming messages addressed to the specified user or group. • **Outbound:** the policy only affects outgoing messages originating from the specified user or group. • **Both:** the policy affects all messages to or from the specified user or group.
Delete	To delete a policy, select its **Delete** check box and click **Submit**.

Creating a New Policy

Click **Add New** to create an Encrypted Message Filtering policy. A window opens, allowing the creation of specific policies.


Apply Encrypted Message Filtering Rule
Use the options below to add a new user, group or domain to which Encrypted Message Filtering rules will apply. From the drop-down list, select the type of user, group or domain, then select the group or domain name from the subsequent drop-down lists or enter the email address in the data field (the correct field or list will be enabled, based upon your first selection). If you want to exclude the user, group or domain from the rules, click the "Exclude" checkbox. Click the appropriate radio button to indicate if you are adding the application for inbound messages, outbound messages, or both.
From the table, select one or more rules to apply by clicking the "Enable" checkbox. At the bottom of the screen, select a default action to be taken for this user, group or domain. Click "Submit" to enter the new application.
Apply To:
Email Address
Select User Group
Select Domain Group
Data:
Exclude:
Direction:
Inbound
Outbound
Both
ID
Monitored Field
Type
Data
Action
Action Value
Notify
Enable
7
Sender
Group
sm
Quarantine Plain Message
0
No
2
Sender
User
user350@sm.ctqa.net
Allow Plain Message
No
Default Action:
Allow Plain Message
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.

The following user input is required:

Field	Description
Apply To	From the pick list, select the type of entity to which the policy will apply. Options are: • Email Address - applies the policy to one individual user (for multiple users, create a group). • User Group - applies the policy to a group consisting of a list of individual users. • Domain Group - applies he policy to a group consisting of a list of domains. • Domain - applies the policy to a single domain (to apply the rule to multiple domains, first create a domain group). • Global - applies the policy to all users. Create any groups required in *Policy Manager > Group Manager > Definition* .

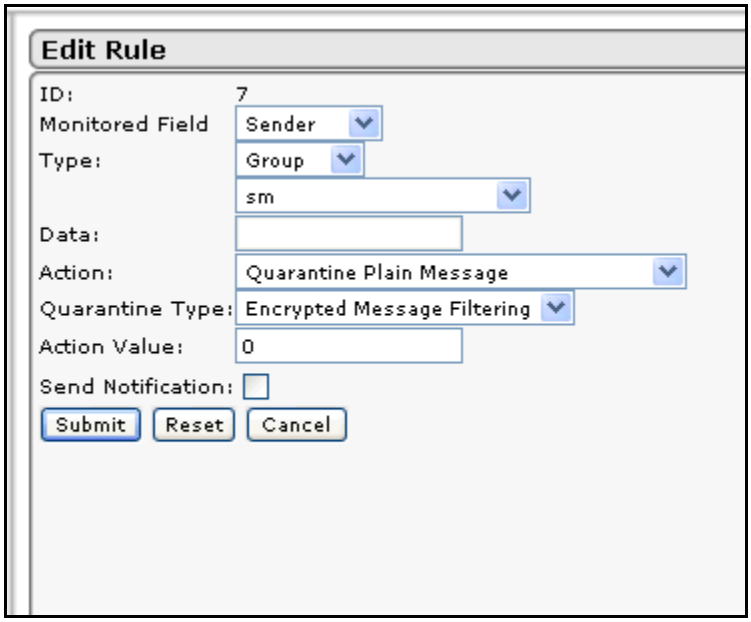
Data	Enter the required data (the email address or domain name) or select the proper group name from the pick lists. The lists will only be enabled if the Apply To type requires the data they contain. The pick list also contains the entry "Global."
Exclude	Select the **Exclude** check box to apply the policy to everyone except the specified user or group. For example, if a rule states that messages originating from dscott@domain.com must be encrypted, and this policy is applied to the Sales group exclusively, then the only users who may receive plain text messages from dscott are members of the Sales group—plain text messages from dscott addressed to anyone else will not be delivered.
Message Direction	Specify the "direction" of mail for which the policy applies. • **Inbound -** the policy only affects incoming messages addressed to the specified user or group. • **Outbound -** the policy only affects outgoing messages originating from the specified user or group. • **Both -** the policy affects all messages to or from the specified user or group.
Table of Rules	***Below the three input fields is a table displaying all Encrypted Message Filtering rules created in* Policy Manager > Encrypted Message Filtering > Manage Rules. *Each row in the table corresponds to a specific rule.***
ID	This column shows the system-generated ID number for each rule. The number is also a hyperlink allowing the Administrator to edit the rule.
Monitored Field	This column identifies the field in the message to be monitored by this rule. Options are: • Sender • Recipient • Subject
Type	This column indicates if the rule will affect messages for a user, group or domain.
Data	This column identifies the user, group, or domain whose messages will be affected by the Encrypted Message Filtering rule. If the rule is based on an individual, an email address will display. If the rule is based on a group, the name of the group will be displayed.
Action	The rule's action is identified. One of six values will display: • Drop encrypted message • Drop plain message • Quarantine encrypted message • Quarantine plain message • Allow encrypted message • Allow plain message
Action Value	This column will display qualifying information related to the rule's action. Only a quarantine action requires qualifying information—a specified number of days the message is to be quarantined.

Enable	Select the **Enable** check box at the right side of the table for each rule to be applied to the specified user or group. Those rules, combined with the Apply, Exclude, and Direction values constitute a single Encrypted Message Filtering "policy."
Default Action	The **Default Action** pick list below the table of Encrypted Message Filtering rules determines whether the specified user or group is allowed or not allowed to receive encrypted messages from anyone else. For example, if the rule states that messages from dscott must be encrypted, and the default action is "Drop encrypted message," then the only encrypted messages the specified user or group may receive are those originating from dscott.

Click **Submit** to save the user input and create the policy. (The policy now displays in the Encrypted Message Filtering Rule Application table in the Web Administration interface.) Click **Add New** again to create additional policies.

Editing an Existing Policy

Clicking on the ID number in the Encrypted Message Filtering Rule Application window opens the Edit Rule screen shown below, populated with the current configuration information for the rule.



Edit the application by modifying the data shown. Click **Submit** to enable the changes.

Field	Description
ID	The policy's ID number shows at the top of the screen, allowing confirmation that changes will impact the right policy. This is not an editable field.
Monitored Field	This field identifies the field in the message to be monitored by this rule. Options are: • Sender • Recipient • Subject
Type	This field indicates if the rule will affect messages for a user, group or domain.

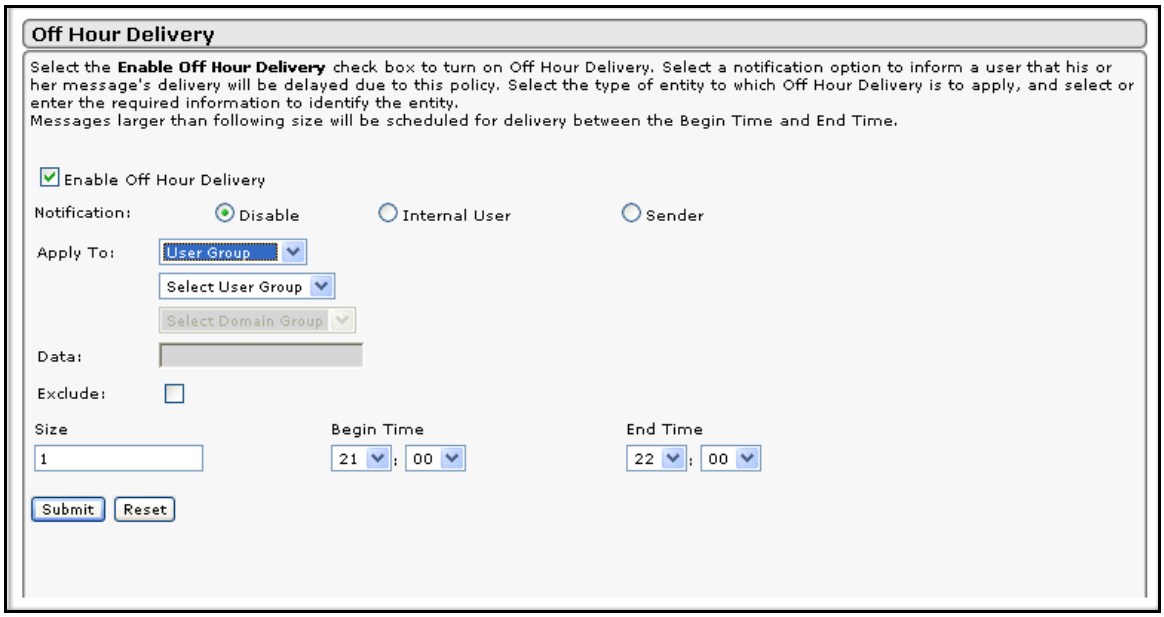
Data	This field identifies the user, group, or domain whose messages will be affected by the Encrypted Message Filtering rule. If the rule is based on an individual, an email address will display. If the rule is based on a group, the name of the group will be displayed.
Action	The rule's action is identified. One of six values will display: • Drop encrypted message • Drop plain message • Quarantine encrypted message • Quarantine plain message • Allow encrypted message • Allow plain message
Quarantine Type	If the quarantine action is configured, this field displays the quarantine type applied by the policy.
Action Value	This column will display qualifying information related to the rule's action. Only a quarantine action requires qualifying information—a specified number of days the message is to be quarantined.
Send Notification	This checkbox, if checked, enables IronMail to send notification as configured whenever the policy is triggered.

Off-Hour Delivery

Administrators may create policies that temporarily delay delivery of large emails until off-peak business hours. This way, bandwidth during peak work hours is not compromised by one or more large file attachments. Messages exceeding the size specified in the Off-Hour Delivery *policy* are temporarily held in the Quarantine Queue.

Administrators also have the ability to set an upper limit on the size of messages that IronMail accepts for delivery. Messages exceeding these limits are not accepted by IronMail.

Off-Hour Delivery is processed in the Mail Monitoring feature; therefore, Mail Monitoring must be set to auto-start and be currently running in order for Off-Hour Delivery policies to function.


Off Hour Delivery
Select the Enable Off Hour Delivery check box to turn on Off Hour Delivery. Select a notification option to inform a user that his or her message's delivery will be delayed due to this policy. Select the type of entity to which Off Hour Delivery is to apply, and select or enter the required information to identify the entity.
Messages larger than following size will be scheduled for delivery between the Begin Time and End Time.
Enable Off Hour Delivery
Notification:
Disable
Internal User
Sender
Apply To:
User Group
Select User Group
Select Domain Group
Data:
Exclude:
Size
Begin Time
End Time
1
21
00
22
00
Submit
Reset

Field	Description
Enable Off Hour Delivery	Select the **Enable Off Hour Delivery** check box to enable Off Hour Delivery. When enabled, IronMail will delay delivery of messages larger than the size specified in the **Size** input field below.
Notification	When messages' delivery is delayed due to this Off Hour Delivery policy, IronMail can generate an email notification indicating the delay. Three choices are available: • Select **Disable** to not generate notifications. • Select **Internal User** to send notifications only to users inside the *network*. Regardless of whether the internal user is the recipient or sender of the message, IronMail will generate a notification to him or her if the Off Hour Delivery policy delayed message delivery. • Select **Sender** to send notifications only to the message sender—the individual identified in the email's FROM address, regardless of whether he or she is inside or outside of the network.
Apply To	From the pick list, select the type of entity to which the policy will apply. Options are: • Email Address - applies the policy to one individual user (for multiple users, create a group). • User Group - applies the policy to a group consisting of a list of individual users. • Domain Group - applies he policy to a group consisting of a list of domains. • Domain - applies the policy to a single domain (to apply the *rule* to multiple domains, first create a domain group). • Global - applies the policy to all users. Create any groups required in *Policy Manager > Group Manager > Definition* .
Data	Enter the required data (the email address or domain name) or select the proper group name from the pick lists. The lists will only be enabled if the Apply To type requires the data they contain. The pick list also contains the entry "Global."
Exclude	Select the **Exclude** check box to apply the policy to everyone except the specified user or group.
Size	Enter a number from 0 to 2000 representing message size in megabytes over which IronMail will delay delivery. A zero ("0") in this field represents "no limit"—IronMail will deliver all messages as they arrive, regardless of size. Note that most email clients must convert binary file attachments to ASCII prior to delivery, resulting in file "bloating," roughly, by a factor of 1.4. Therefore, if Windows Explorer reports a file size of 10 MB, the email client application will convert it to an approximately 14 MB file. Users may think they are sending a file smaller than the Off-Hour Delivery limit, when, in fact, it may be too large.
Begin Time	Use the **Hour** and **Minute** pick lists to set the time when IronMail should begin delivering large messages that have accumulated for Off-Hour Delivery.
End Time	Use the **Hour** and **Minute** pick lists to set the time when IronMail should stop delivering large messages that have accumulated for Off-Hour Delivery.

If IronMail does not finish delivering all large messages before the End Time arrives, unsent messages remain in the queue until the next Begin Time. Administrators, however, may manually "push" messages out of the queue.

Filtering Message Attachments

Attachment Filtering

Attachments, including files such as Word documents, PDFs, executable files, etc., that are included with (attached to) email messages can carry threats like spam or viruses. IronMail's Attachment Filtering functionality allows the Administrator to configure and apply rules and policies to prevent these attachments from entering the *network* and to circumvent the threats.

Creating Attachment Filtering policies is a two-step process. First, Attachment Filtering *"rules"* must be created specifying file types and an IronMail response to each type of file. Second, the Attachment Filtering rules must be applied to users or groups of users—thereby creating Attachment Filtering *"policies*."

The Attachment Filtering hyperlink in the left navigation frame expands to offer Manage Rules and Apply Rules sub-menus.

In addition to regular attachments, IronMail also performs attachment filtering on the contents of attached zip files. When text is extracted from associated zip files, IronMail subjects this text to content filtering. Zip files contained in attached zip files are filtered down to four levels of zipping.

The processing order within Attachment Filtering is illustrated below.

<table>
<tr><th colspan="3">Attachment Filtering</th></tr>
<tr><td></td><td>Attachment Filtering Policy</td><td></td></tr>
<tr><td>From Previous

Queue</td><td>Re-Route - do not proceed to next policy
Drop Message - do not proceed to next policy
Quarantine - proceed to next policy
Secure Delivery - proceed to next policy
Forward as Attachment - proceed to next policy
Drop Part - proceed to next policy
Subject Re-write - proceed to next policy
Copy as Attachment - proceed to next policy
Copy - proceed to next policy
Rename - proceed to next policy
Log - proceed to next policy
Pass-Through - proceed to next policy</td><td>To Next

Queue</td></tr>
</table>

Multiple Rules

Whenever a message conforms to multiple rules, more than one action may be performed on that message. In some situations, not all actions can be performed.

- Policy attribute comparison is used to resolve conflicting actions. In the comparison, a system-defined policy supercedes a user-defined policy, a policy applied to a user supercedes a policy applied to a group, and a higher action code supercedes a lower one.
- If both secure delivery and forward actions could apply to a message, secure delivery has precedence because the forward action could cause the original message to be deleted and the message will not be securely delivered. Other actions can be applied along with secure delivery.
- Policy attribute comparison is performed to resolve the conflict above when the actions belong to different policies; just action codes are compared when both rules belong to the same policy.
- When multiple quarantine rules with finite quarantine days may be applied, policy attribute comparison is used to choose one of them. In this case, the quarantine period is compared instead of the action code.
- Policy attribute comparison is performed to resolve the conflicts that will occur when drop part and rename actions are defined on the same attachment extension or filename. These are part-level actions, so only one can be applied. The same is true if the actions are pass-through and drop part.
- Policy attribute comparison is done to resolve conflicts that will arise from defining two rename actions on the same extension. The part can only be renamed to one or the other of the action data values.
- Policy attribute comparison is used between two rules when one of them is either a reroute or drop *rule*, or a quarantine forever, and the other rule is an action in (4) or (5). A copy action in a policy applied to a user supercedes a reroute action applied to a group.
- Policy attribute comparison is performed between two rules when either of them is one of the following:
    - Reroute rule,
    - Drop rule, or
    - Quarantine forever.
- If one of the actions is a reroute or drop rule or a quarantine forever, the one action will be performed and all other actions will be ignored because the message will no longer be available for additional actions.

Note on File Types within a Zip file

Zip files contained in attached zip files are filtered down to four levels of zipping. Policy rules govern the way emails are handled depending on the types of files contained in attached zip files. Files inside a zip file can be filtered by specifying a secondary action for that attachment type. Although IronMail does not modify the zip file, it can treat the message and zip attachment as a whole based on the inside attachment and quarantine or drop the message based on a rule applied to the zip contents.

Administrators can define policy rules that control the way emails are handled depending on the type of files that are contained in attached zip files. However, IronMail cannot perform the Drop Part or Rename actions on files within a zip file. Instead, administrators can define alternative actions based on specific file types within an attached zip file using the Add New Rule window.

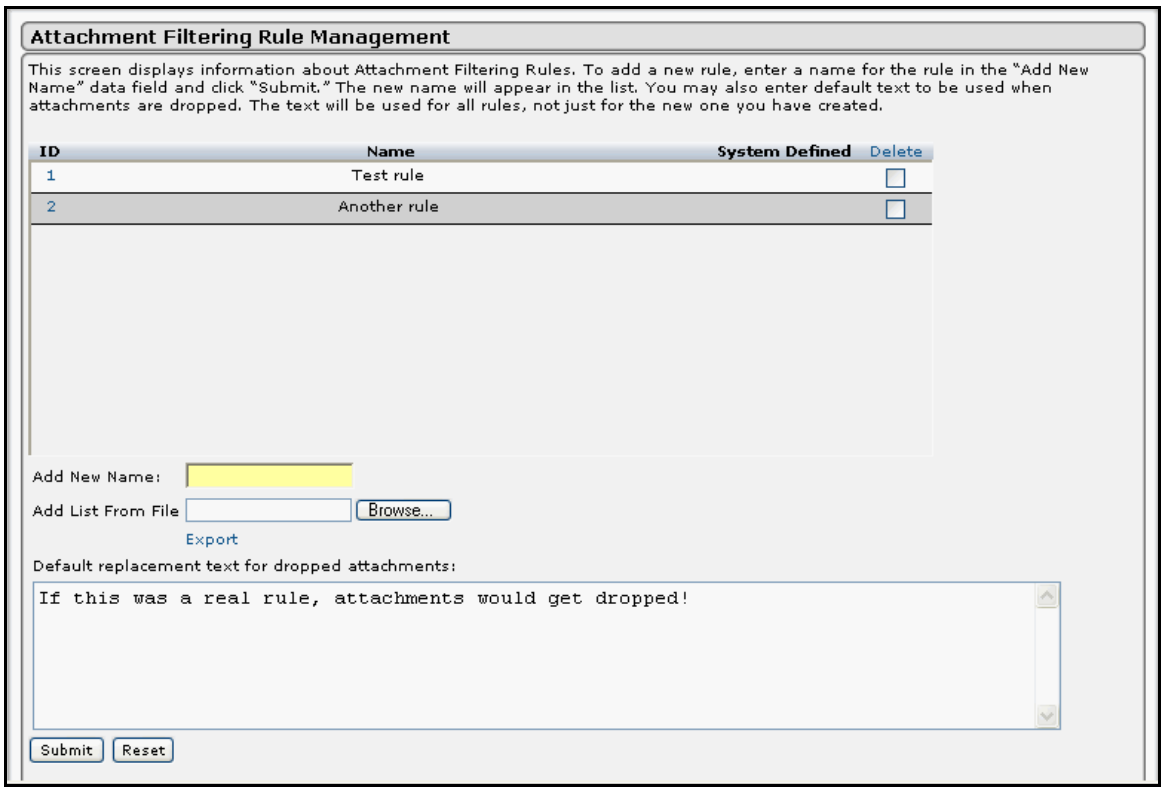
These alternate actions are only available if the Drop Part and Rename primary actions are selected on the window.

Actions such as Drop Message or Quarantine must be applied to the entire message since IronMail cannot just Drop or Quarantine specified file types within the zip file. For example, if an administrator creates a rule to drop .exe files, IronMail drops the entire message with the attached zip file containing the .exe file, even if the zip also contains html, txt, or other file types.

In addition, the IronMail Virus Engine can scan the contents within a zip file down to sixteen levels of zipping. If a virus is detected and it can be cleaned, this cleaning is performed. If it cannot be cleaned, action is taken on the entire zip part or the entire message.

Manage Rules

Rules that link specific file types with IronMail responses are created in the Attachment Filtering Rule Management window. This window contains a table of rules, empty until rules have been created.


Attachment Filtering Rule Management
This screen displays information about Attachment Filtering Rules. To add a new rule, enter a name for the rule in the "Add New Name" data field and click "Submit." The new name will appear in the list. You may also enter default text to be used when attachments are dropped. The text will be used for all rules, not just for the new one you have created.
ID
Name
System Defined
Delete
1
Test rule
2
Another rule
Add New Name:
Add List From File
Browse...
Export
Default replacement text for dropped attachments:
If this was a real rule, attachments would get dropped!
Submit
Reset

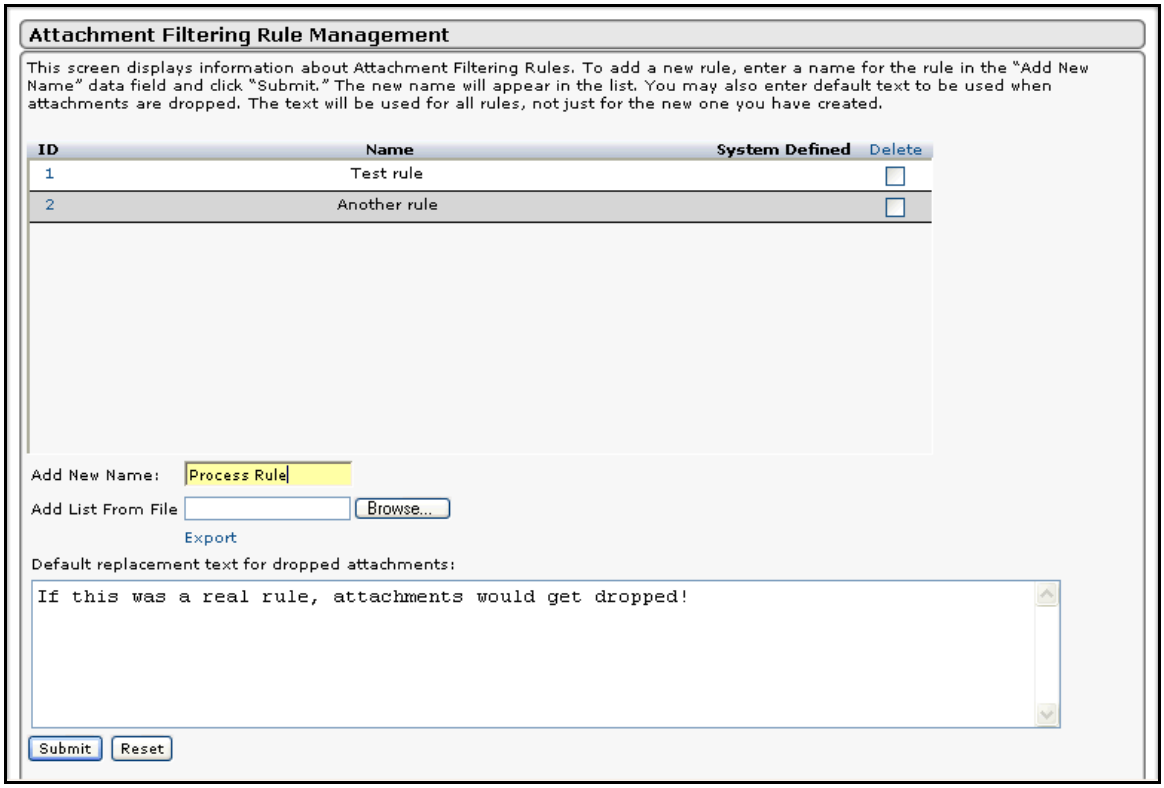
The following information is displayed in the table:

ID	This column displays the unique ID number that IronMail generates for each Attachment Filtering rule. Whenever a *policy* is enforced, IronMail's reports or logs will provide information about the message, and the specific Attachment Filtering Rule ID responsible for causing IronMail to act on the message. Rule ID numbers are serially incremented. If a rule is deleted, IronMail does not re-use its ID number. The Rule ID is also a hyperlink opening a window in which the rule may be edited.
Name	This column reports the rule's human-friendly name. (When rules are created, the administrator is prompted to "name" it.)

System Defined	An "X" in this column indicates that the rule was generated by the system, rather than by the Administrator or user.
Delete	Selecting the **Delete** check box for a rule and clicking **Submit**, deletes a rule from the table. (When all the rules on which an Attachment Filtering policy is based are deleted, the policy is deleted from the *Attachment Filtering > Attachment Filtering Rule Application* table of policies.)

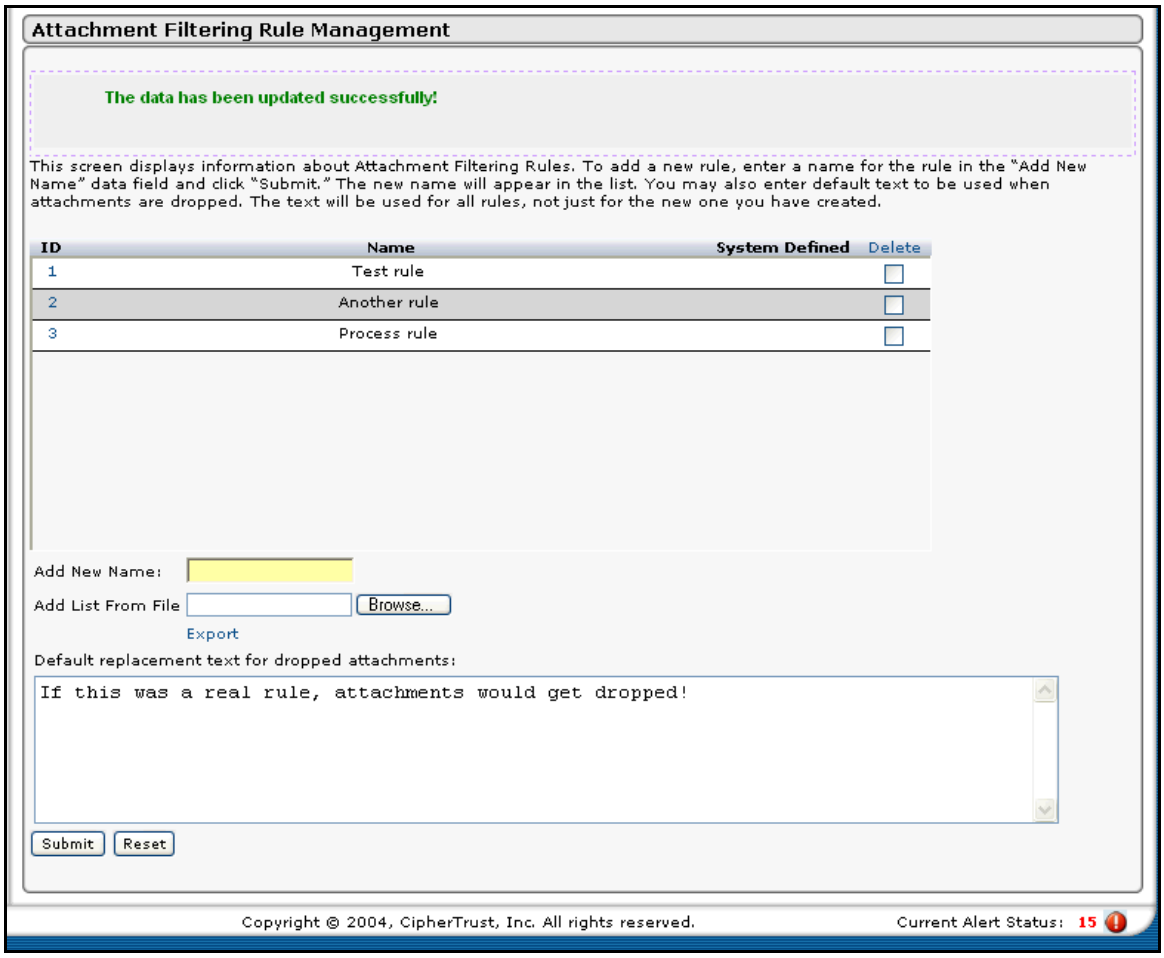
Adding a New Rule

An **Add New Name** input field appears below the table of rules. Enter a descriptive name for a rule.


Attachment Filtering Rule Management
This screen displays information about Attachment Filtering Rules. To add a new rule, enter a name for the rule in the "Add New Name" data field and click "Submit." The new name will appear in the list. You may also enter default text to be used when attachments are dropped. The text will be used for all rules, not just for the new one you have created.
ID
Name
System Defined
Delete
1
Test rule
2
Another rule
Add New Name:
Process Rule
Add List From File
Browse...
Export
Default replacement text for dropped attachments:
If this was a real rule, attachments would get dropped!
Submit
Reset

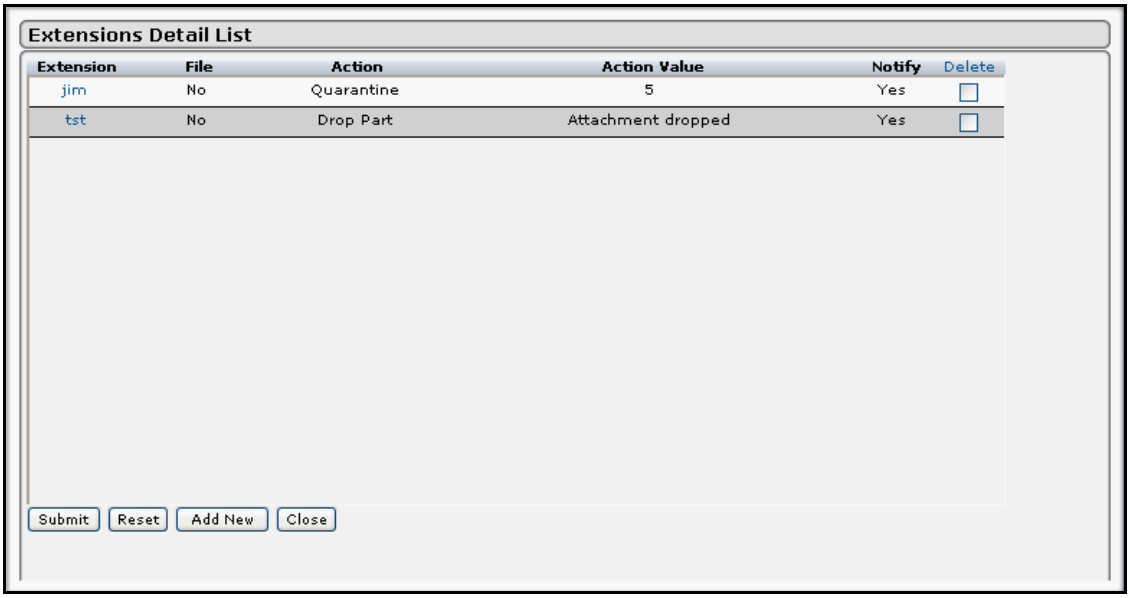
Below the **Add New Name** input field is a **Default Replacement Text** message field. Use this field to provide a generic statement explaining to affected users that a file attachment has been dropped.

Clicking **Submit** will add the new rule and/or text to the Attachment Filtering Rule Management window.


Attachment Filtering Rule Management
The data has been updated successfully!
This screen displays information about Attachment Filtering Rules. To add a new rule, enter a name for the rule in the "Add New Name" data field and click "Submit." The new name will appear in the list. You may also enter default text to be used when attachments are dropped. The text will be used for all rules, not just for the new one you have created.
ID
Name
System Defined
Delete
1
Test rule
2
Another rule
3
Process rule
Add New Name:
Add List From File
Browse...
Export
Default replacement text for dropped attachments:
If this was a real rule, attachments would get dropped!
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 15

Completing or Editing a Rule

Once the rule name has been added to the table, completing the new rule (or editing an existing rule) requires the user to click the rule's ID hyperlink. This opens the Extension Detail List, which shows all the extensions (attachment types) associated with the specific rule.



The screen displays the following information:

Field	Description
Extension	The column lists the extension abbreviation or filename for the specific attachment.
File	An "X" in this column indicates that the attachment is a file, not simply an extension.
Action	The items in this column show the action IronMail is to take if the particular extension is detected in an email attachment
Action Value	If other information, such as an *IP address* or a number of days a message should remain in quarantine, is required for an action, that value will appear in this column.
Notify	A "Yes" in this column indicates that IronMail should send notification that the rule has been triggered, as configured in Policy Manager > Mail Notification.
Delete	To delete an extension or filename from the list, click the Delete checkbox and then click **Submit**. All extensions may be deleted at one time by clicking the Delete hyperlink.

Adding a New Extension

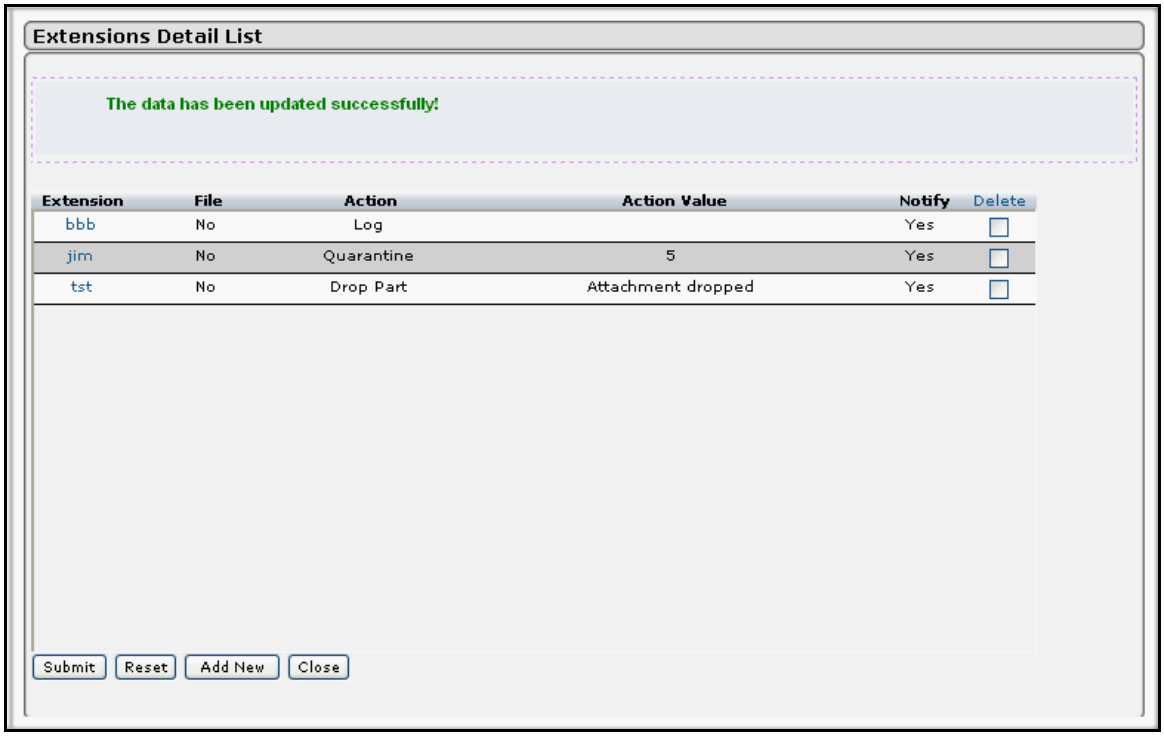
The "Add New" Button at the bottom of the screen opens the Add New Rule window, where one can add new extensions or filenames to the rule or edit those that already exist.

Field	Description
Extension/Filename	Enter a file name or file extension in the **Extension/Filename** input field. When entering a file extension, do not enter the dot-prefix separating the file name from its extension. (Examples of valid extension entries are: doc, xls, rtf, gif, jp.,zip) When IronMail parses and reads an email's *MIME* part identifying file attachments, it looks for the period in the attachment filename and reads to the right of the period.
File	If a file name was provided in the **Extension/Filename** input field above, IronMail must be explicitly told to look for a file, since some file systems do not use dot-delimiters in their file-naming scheme. Click the checkbox to indicate this attachment is a file.
Action	IronMail can perform one of eleven actions when it encounters a message with a specified file or file type. Select an action from the **Action** pick list: • **Secure Delivery:** IronMail will always deliver messages to or from the specified user, group, or domain securely. First, IronMail will attempt to deliver the message using S/MIME. If S/MIME is not supported, IronMail will see if PGP certificates have been installed, and attempt that secure method. If neither is available or unsupported by the other mail server, IronMail will attempt a *SSL* delivery. And if none of these can be supported, IronMail will deliver the message via HTTPS—its Secure Web Delivery. • **Subject re-write:** IronMail will prepend the message's Subject line with a text string provided in the **Action Value** input field below. For example, messages with ".exe" extensions can have their Subject line prepended with the text "Use CAUTION when opening the attached file!" • **Drop message:** IronMail will drop the entire message. Administrators may elect to send an IronMail-generated email, indicating that the message was dropped because of this Attachment Filtering rule. However, IronMail will only do so if **Send Notification** is enabled below, and also enabled in *Policy Manager > Attachment Filtering > Apply Rules*. *There is an inherent risk when dropping text files.* • **Log:** IronMail will deliver the message with the specified attachment, but record in its Daily Policy Compliance Report that the message matched the conditions of the Attachment Filtering rule. (The Daily Policy Compliance Report is viewed in *Monitoring > Reports/Log Files > Reports*. Note that the "Daily Policy Compliance—Detailed" report must be manually enabled in *Monitoring > Reports/Log Files > Reports Configuration* in order for the log action to function. • **Re-route:** IronMail will re-route the message to a specified machine for additional processing. If the re-route action is specified, the IP address of the server must be entered in the **Action Value** input field below. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Value** field indicating how many days the message remains in the queue before returning to

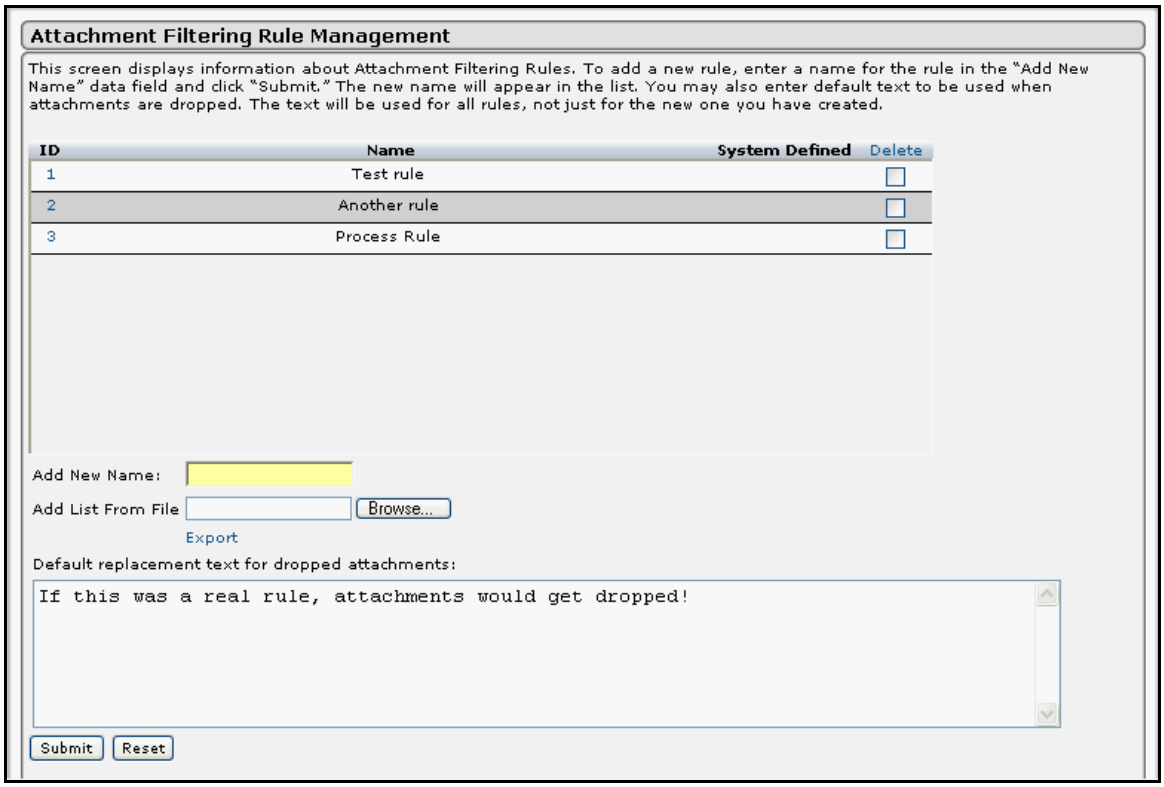
	the normal mail flow. • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Value** field below. • **Drop part:** IronMail will drop just the file attachment. If a text string—i.e., a user-defined message—is entered in the **Action Value** input field below, the message is appended to the email as a text file attachment. The message may state, for example, that files of the specified type are not allowed to enter the *network* via email attachments. **Note:** Only the specified attachment types will be dropped. • **Rename:** IronMail will rename the file or file extension. When this action is selected, a text string must be entered in **Action Value** input field below. For example, executable files may have their extensions renamed from "exe" to "ex?" • **Copy as attachment:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the **Action Value** column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Copy Message:** IronMail will deliver the original message but send a copy of the message to an alternate address. This action inserts the alternate address in the RFC821 Cc: header—it does not display in the RFC822 Cc: header. • **Pass through:** IronMail allows messages containing the specified file name or file type to be delivered. This action is selected in order to create a policy that allows a user or group to receive specific file types, and have *all other files types blocked*. That is, instead of creating a policy that blocks specific file types, this allows the creation of a policy that allows only specified files to be sent or received and blocks all others.
Action Value	Some actions require qualifying information. • **Subject re-write:** this action requires a text string. The text string may be any printable character up to 256 characters long. For example, messages with ".exe" extensions can have their Subject line prepended with the text "Use CAUTION when opening the attached file!" • **Re-route:** this action requires a valid IP address. • **Quarantine:** this action requires a numeric value from 0 to 15. The number represents how many days the message will be quarantined before IronMail delivers it. For example, if a message is received at 12:30 PM on Wednesday and is quarantined for two days, IronMail will return the message to its regular mail flow at 12:30 PM Friday, and any queues that have not yet processed the message will do so before final delivery. A zero ("0") value, however, indicates "Do Not Deliver!" Any message with a quarantine value of zero will be automatically deleted according to the Cleanup Schedule for Quarantine Data (*System > Cleanup Schedule*). • **Forward Message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. Do not enter spaces between commas and subsequent email addresses. • **Drop part:** this action requires a text string. The string may contain

	any printable character, and up to 256 characters long. • **Rename:** this action requires a text string and may contain any printable character, and up to 256 characters long. • **Copy message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. Do not enter spaces between commas and subsequent email addresses.
Alternative Action	Select the alternate action IronMail should perform if a file with this extension or file name is detected.
Alternative Action Value	Provide values relevant for the Alternate Action if one is specified. For example, the Quarantine action needs to know how many days to quarantine a message.
Quarantine Type	If the Quarantine action is selected in the **Action** pick list above, this **Quarantine Type** pick list becomes enabled. It displays the default quarantine queues, and any other queues that were manually created. Select a queue where messages with the specified file attachments will be sent.
Send Notification	An IronMail-generated email may be sent when a File Attachment policy affects a message. The text of the notification is configured in *Policy Manager > Mail Notification*.

Click **Submit** to record the information entered. The new extension will appear on the Extensions Detail List at the top of the list.



When all the information has been entered or edited and saved, the Attachment Filtering Rule Management screen shows the complete list of available rules.


Attachment Filtering Rule Management
This screen displays information about Attachment Filtering Rules. To add a new rule, enter a name for the rule in the "Add New Name" data field and click "Submit." The new name will appear in the list. You may also enter default text to be used when attachments are dropped. The text will be used for all rules, not just for the new one you have created.
ID
Name
System Defined
Delete
1
Test rule
2
Another rule
3
Process Rule
Add New Name:
Add List From File
Browse...
Export
Default replacement text for dropped attachments:
If this was a real rule, attachments would get dropped!
Submit
Reset

It is up to the discretion of administrators whether or not to provide a Default Replacement Text message. If a message is not provided in the **Default Replacement Text** message field, files dropped because of the default drop action will simply be dropped with no notification to end users.

Click **Submit** to save user input. Click **Close** to close the Edit Extension List window. When returned to the secondary Rule Detail List window, click **Add New** again to add additional files or file types to the rule.

Attachment Filtering rules are not active until they become policies when rules are applied to users or groups. Navigate to *Policy Manager > Attachment Filtering > Apply Rules* to make Attachment Filtering policies.

Adding Lists in Attachment Filtering

Import files for attachment filtering should contain one or more lines in the format:

```
rule_name|file_ext_name|is_file|action|action_value|alter
nat
ive_action|alternative_action_value|quarantine_type|notif
ica
tion
```

Where **rule_name** is a required field and is an alpha string representing the "name of the rule" (e.g., "my blocked files").

Where **file_ext_name** is a required field and is an alpha string representing either a file *extension* or *filename*. The period (.) extension-delimiter is not allowed when entering an extension—user interface validation prohibits this string from beginning with a period.

Where **is_file** is a required field that accepts the following values:
0 = extension
1 = file

Where **action** is a required field and represents the exact name of Attachment Filtering Policy's actions (e.g., quarantine, copy, drop message)

Where **action_value** is a required field and represents the qualifying information related to the action (e.g., a **copy** action requires an email address as the **action_data**, and a **quarantine** action requires a number indicating how many days a message is to be quarantined)

Where **alternative_action** is a required field if the "action" field is "drop part" or "rename." For all other actions this field should be empty, represented by two pipe symbols with nothing inside them (||).

Where **alternative_action_value** is a required field if the "alternative_action" field is populated with data. This field may contain any action except "drop part" or "rename."

Where **quarantine_type** is a required field if the "action" field contains a **quarantine** action. This field must contain the exact name of an existing Quarantine Queue.

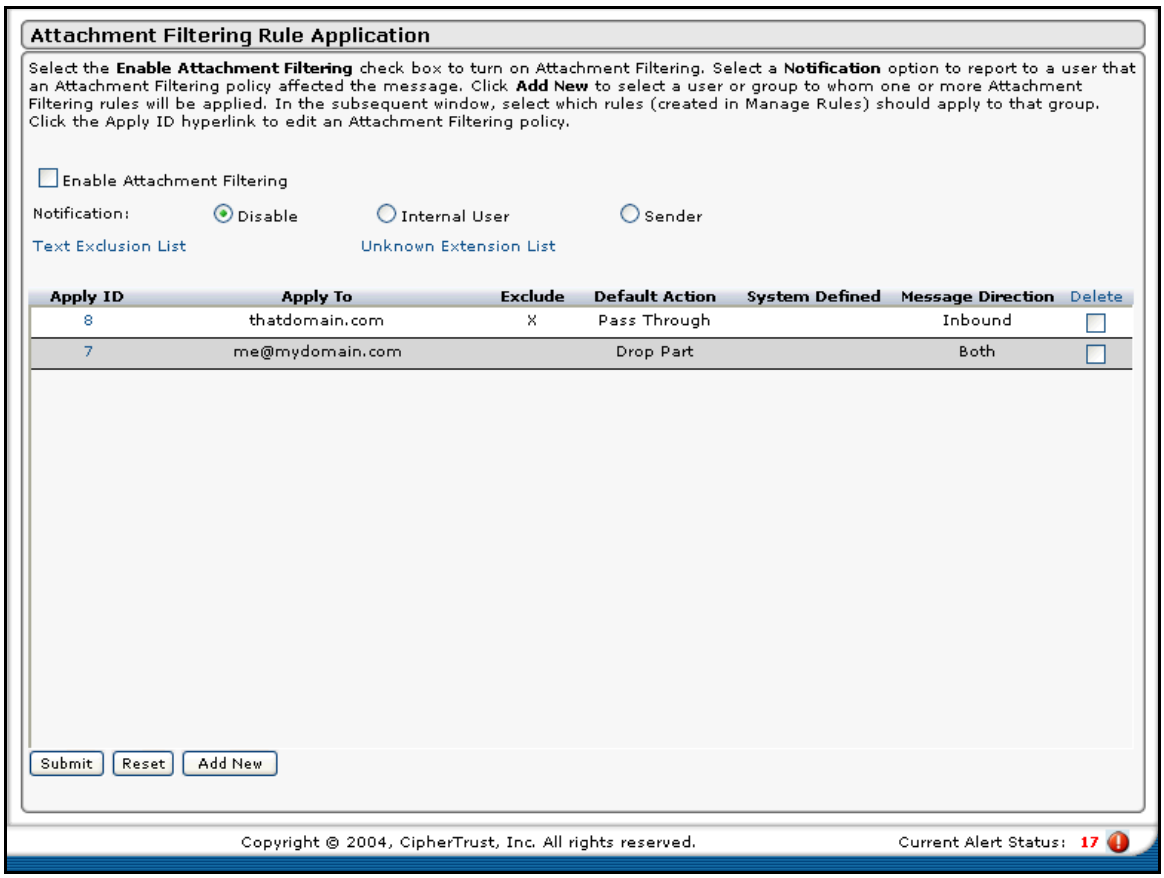
Where **notification** is a required field that accepts the following values:
0 = not enabled
1 = enabled

Some good examples of attachment filtering policies in an import file are:

```
blocked|exe|0|quarantine|0|||CFQ attachment filtering|1
allowed|pdf|0|Pass Through|||||0
dropped|*scr|1|Drop Part|Screensaver files are not
allowed this

     network.|Quarantine|0|CFQ screensavers|0
```

Apply Rules

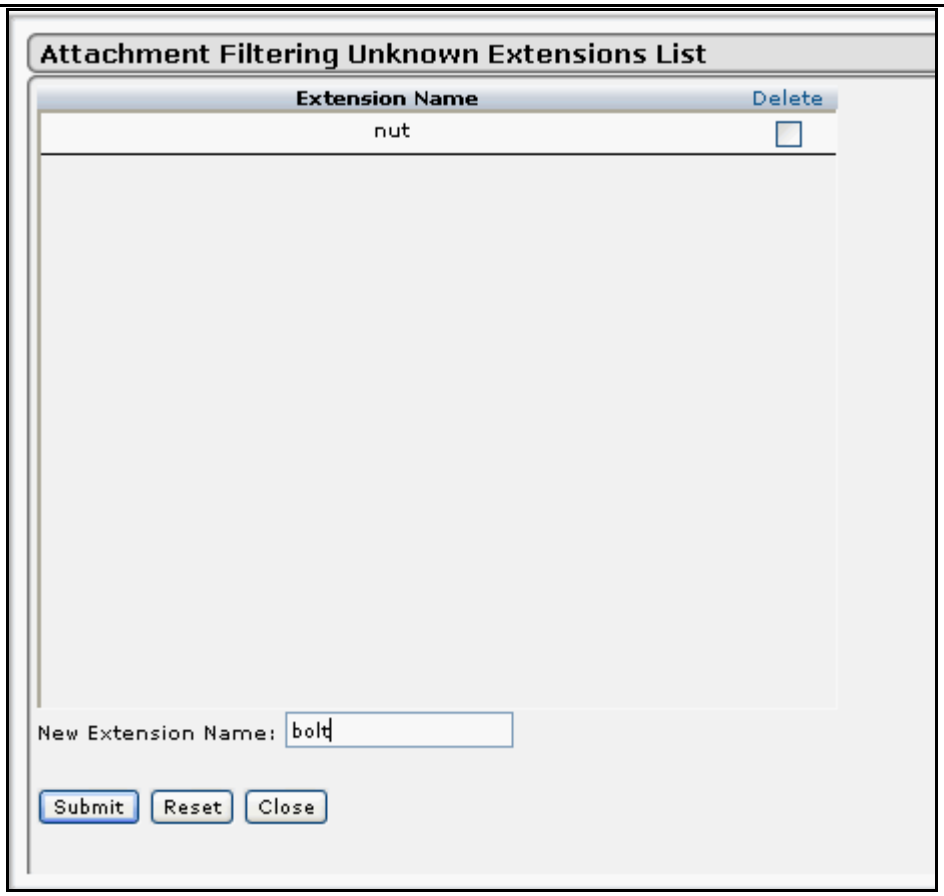
Attachment Filtering *rules* are created in *Policy Manager > Attachment Filtering > Manage Rules*, but they do not become active until they are applied to specific users or groups. Only after the rules are converted into Attachment Filtering *policies* in this window will IronMail take the specified actions for messages (identified in the *rule*) processed by IronMail.


Attachment Filtering Rule Application
Select the Enable Attachment Filtering check box to turn on Attachment Filtering. Select a Notification option to report to a user that an Attachment Filtering policy affected the message. Click Add New to select a user or group to whom one or more Attachment Filtering rules will be applied. In the subsequent window, select which rules (created in Manage Rules) should apply to that group. Click the Apply ID hyperlink to edit an Attachment Filtering policy.
Enable Attachment Filtering
Notification:
Disable
Internal User
Sender
Text Exclusion List
Unknown Extension List
Apply ID
Apply To
Exclude
Default Action
System Defined
Message Direction
Delete
8
thatdomain.com
X
Pass Through
Inbound
7
me@mydomain.com
Drop Part
Both
Submit
Reset
Add New
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 17

The first configuration area on the page is headed **Setting**, offering two options:

Enable Attachment Filtering	Select the **Enable Attachment Filtering** check box to enable, or "turn on," Attachment Filtering. If enabled, IronMail will enforce the Attachment Filtering policies listed in the table below. Note that Attachment Filtering policies are enforced, or processed, in the Content Filtering Queue, one of IronMail's queue subsystems. Therefore, the Content Filtering Queue must be set to Auto-Start, Running, and assigned a "queue position." The Web Administration user interface will allow **Enable Attachment Filtering** to be selected even if the Content Filtering Queue is not currently running, but the Attachment Filtering policies will not be enforced until the queue is enabled.
Notification	When Attachment Filtering rules were created in the *Policy Manager > Attachment Filtering > Manage Rules* page, an option provided for a notification to be generated if the rule acted upon a message. The notification setting here relates to that option. Three qualifying choices are available: • Select **Disable** to override the notification setting within individual Attachment Filtering rules. If this radio button is selected, IronMail will not generate any notifications if Attachment Filtering rules affect a message. • Select **Internal User** to send notifications only to users inside the *network*. Regardless of whether the internal user is the recipient or sender of the

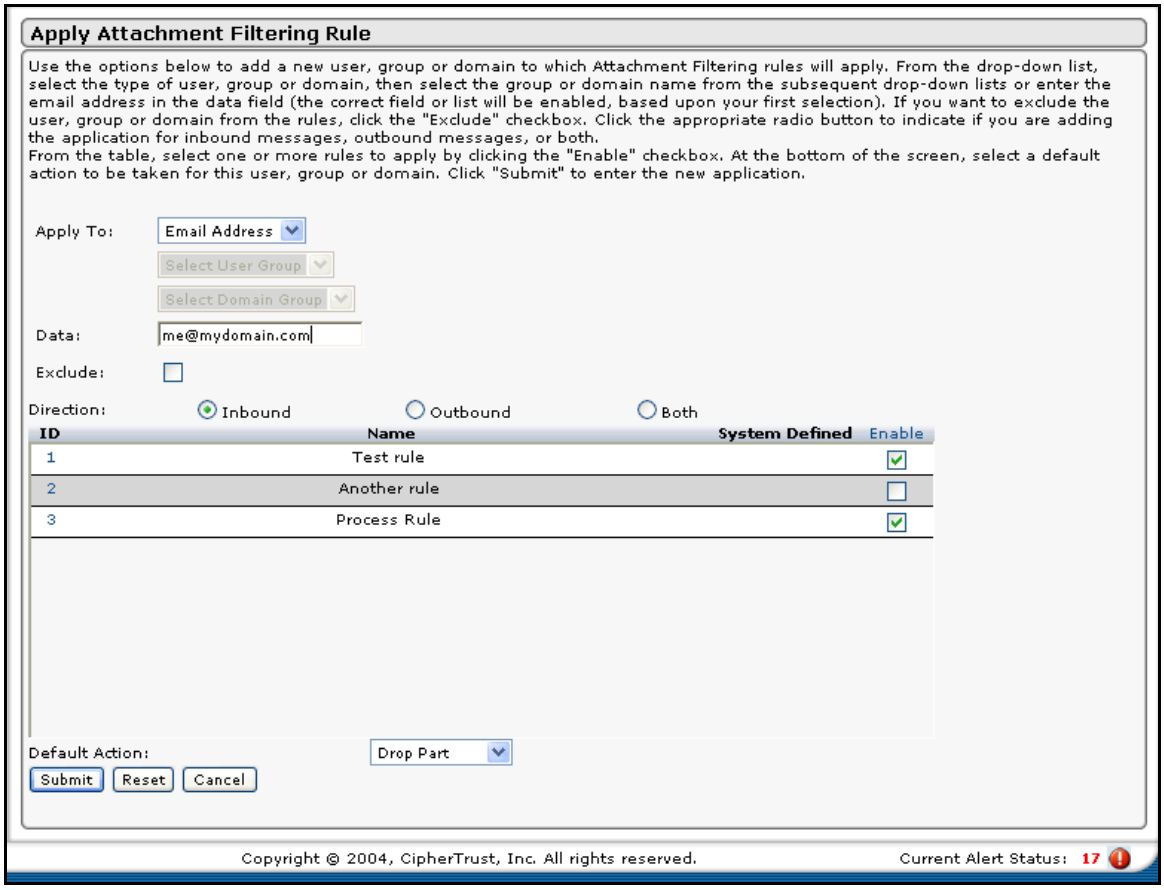
	message, IronMail will generate a notification to him or her if an Attachment Filtering policy took an action on the message. • Select **Sender** to send notifications only to the message sender—the individual identified in the email's FROM address, regardless of whether he or she is inside or outside the network.
Text Exclusion List	IronMail recognizes 7-bit ASCII formatted files (typically files with TXT as their file extension), even if the file contains an extension *other than TXT*. If an Attachment Filtering policy is created for TXT files, IronMail will enforce the policy on all ASCII text file attachments, whether their extension is TXT, EML, VCF, DAT, LOG, or any other arbitrary extension. To exclude a 7-bit ASCII file from being acted upon by a policy that addresses TXT files, enter its file extension in the Text Exclusion List. To add a file type to the Attachment Filtering File Extension List, click the **Text Exclusion List** hyperlink. A secondary browser window opens, allowing the entry of file extensions. Enter a file extension in the New Extension Name input field and click Submit. Repeat for all extensions for which you want to explicitly create Attachment Filtering rules. These extension will *not* be treated as "text" for the enforcement of Attachment Filtering policies.
Unknown Extension List	When filtering attachments, IronMail reads the file name extension and compares it with a bypass list. If the file type is present on the list, the attachment is treated according to filtering rules for the extension. The Attachment Filtering Unknown Extension List window enables an Administrator to add to the list of extensions that will NOT be treated as unknown. If the extension is not in the bypass list, the attachment is treated as an unknown and an action is taken if a rule was set up for the .unk extension.

	 To add a file type to the Attachment Filtering Unknown Extension List, click the **Unknown Extension List** hyperlink. Enter a file name extension in the New Extension Name input field and click **Submit**. To delete extensions, select them in the **Delete** column, or click the Delete heading to select all extensions. Click **Submit** to perform the deletion
Apply ID	IronMail identifies each policy with a unique, serially incrementing ID number. Note that IronMail's serial numbers span all policies processed by the Content Filtering Queue. Thus, the ID numbers for Attachment Filtering, Content Filtering, and Message Stamping policies will not be duplicated—each time a policy within any of those three program areas is created, it is assigned the next higher number. IronMail's logs and Daily Policy Compliance Reports will report the policy ID number when messages match the criteria of specific policies. The ID number is also a hyperlink that opens a secondary browser window in which the policy may be edited.
Apply To	This column reports the individual or group to whom the specific policy applies.
Exclude	A mark in the **Exclude** column indicates that the policy applies globally to everyone *except* the specified individual or group.
Default Action	This column reports one of two values: Pass through or Drop. • **Pass through:** all file attachments other than the one(s) specified in the rule are allowed to be sent/received. • **Drop:** all file attachments other than the one(s) specified in the rule are dropped.

System Defined	This column indicates whether the policy was generated by another IronMail process. For example, IronMail's Anomaly Detection Engine is capable of creating rules that drop certain types of file attachments.
Message Direction	This column indicates the "direction" of mail for which the policy applies. One of three values will display: • **Inbound:** the policy only affects incoming messages addressed to the specified user or group. • **Outbound:** the policy only affects outgoing messages originating from the specified user or group. • **Both:** the policy affects all messages to or from the specified user or group.
Delete	To delete a policy, select its **Delete** check box and click **Submit**. Note that system-generated policies may not be deleted from this table. To delete a system-generated policy, navigate to *Policy Manager > Attachment Filtering > Manage Rules* and delete the specific rules that comprise the Attachment Filtering policy. Once all the rules are deleted, the policy will automatically be deleted from the table.

Adding a New Application

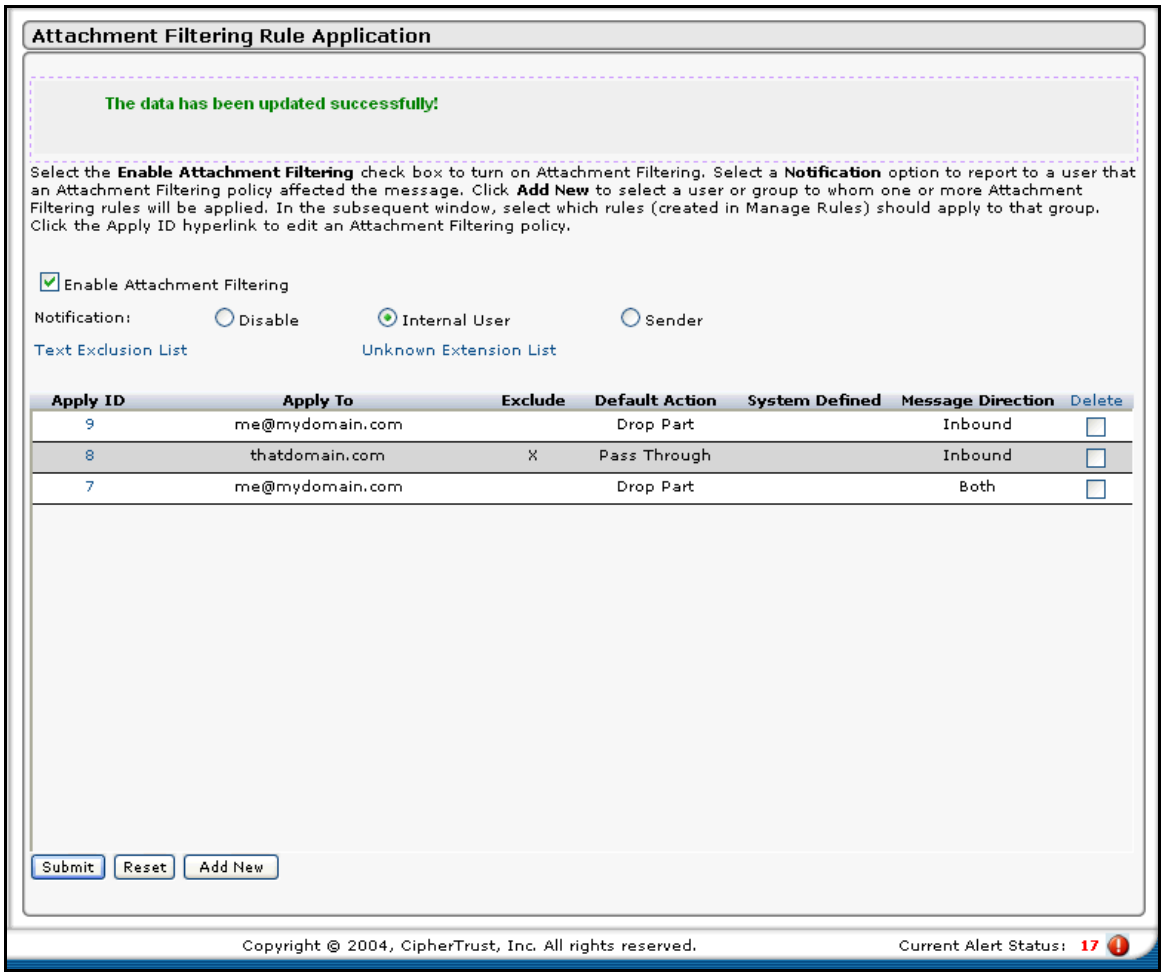
Click **Add New** to generate a new policy based on specific rules created in *Policy Manager > Attachment Filtering > Manage Rules*. An Apply Attachment Filtering Rule secondary browser window opens.


Apply Attachment Filtering Rule
Use the options below to add a new user, group or domain to which Attachment Filtering rules will apply. From the drop-down list, select the type of user, group or domain, then select the group or domain name from the subsequent drop-down lists or enter the email address in the data field (the correct field or list will be enabled, based upon your first selection). If you want to exclude the user, group or domain from the rules, click the "Exclude" checkbox. Click the appropriate radio button to indicate if you are adding the application for inbound messages, outbound messages, or both.
From the table, select one or more rules to apply by clicking the "Enable" checkbox. At the bottom of the screen, select a default action to be taken for this user, group or domain. Click "Submit" to enter the new application.
Apply To:
Email Address
Select User Group
Select Domain Group
Data:
me@mydomain.com
Exclude:
Direction:
Inbound
Outbound
Both
ID
Name
System Defined
Enable
1
Test rule
2
Another rule
3
Process Rule
Default Action:
Drop Part
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status:
17

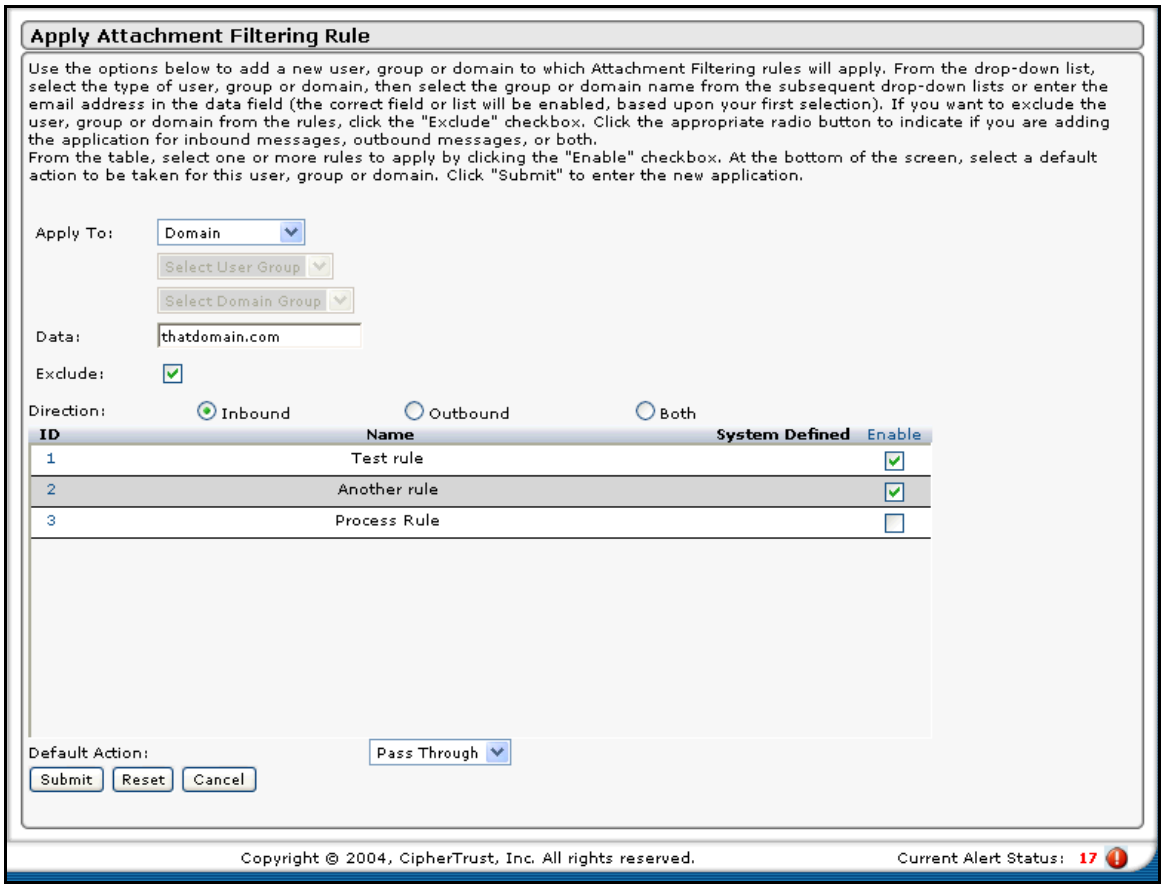
Provide the following input:

Field	Description
Apply To	From the pick list, select the type of entity to which the policy will apply. Options are: • Email Address - applies the policy to one individual user (for multiple users, create a group). • User Group - applies the policy to a group consisting of a list of individual users. • Domain Group - applies he policy to a group consisting of a list of domains. • Domain - applies the policy to a single domain (to apply the rule to multiple domains, first create a domain group). • Global - applies the policy to all users. Create any groups required in *Policy Manager > Group Manager > Definition* .
Data	Enter the required data (the email address or domain name) or select the proper group name from the pick lists. The lists will only be enabled if the Apply To type requires the data they contain. The pick list also contains the entry "Global."
Exclude	Select the **Exclude** check box to apply the policy to everyone except the specified user or group.
Direction	Specify the "direction" of mail for which the policy applies. • **Inbound -** the policy only affects incoming messages addressed to the specified user or group. • **Outbound -** the policy only affects outgoing messages originating from the specified user or group. • **Both -** the policy affects all messages to or from the specified user or group.
Table of Rules	***The lower portion of the screen lists all the rules available to be applied through the new policy.***
ID	This column lists the system-generated ID for the new application. These IDs are sequentially created. If an application is deleted, the ID number is NOT used again.
Name	This column shows the rule names that were entered when the rules were created or last edited.
System Defined	An "X" in this column indicates the rule was generated by another IronMail function.
Enable	Clicking this check box enables the specific rule for this application.
Default Action	From the pick list at the bottom of the screen, choose the default action IronMail is to take if any rule in this application is triggered.

Click **Submit** to record the information. The policy now displays in the Attachment Filtering Rule Application screen in the Web Administration interface. Click **Add New** again to create additional policies.


Attachment Filtering Rule Application
The data has been updated successfully!
Select the Enable Attachment Filtering check box to turn on Attachment Filtering. Select a Notification option to report to a user that an Attachment Filtering policy affected the message. Click Add New to select a user or group to whom one or more Attachment Filtering rules will be applied. In the subsequent window, select which rules (created in Manage Rules) should apply to that group. Click the Apply ID hyperlink to edit an Attachment Filtering policy.
Enable Attachment Filtering
Notification:
Disable
Internal User
Sender
Text Exclusion List
Unknown Extension List
Apply ID
Apply To
Exclude
Default Action
System Defined
Message Direction
Delete
9
me@mydomain.com
Drop Part
Inbound
8
thatdomain.com
X
Pass Through
Inbound
7
me@mydomain.com
Drop Part
Both
Submit
Reset
Add New
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 17

When the applications of Attachment Filtering rules have been configured, the Apply Attachment Filtering Rule screen shows all the applications that have been established.


Apply Attachment Filtering Rule
Use the options below to add a new user, group or domain to which Attachment Filtering rules will apply. From the drop-down list, select the type of user, group or domain, then select the group or domain name from the subsequent drop-down lists or enter the email address in the data field (the correct field or list will be enabled, based upon your first selection). If you want to exclude the user, group or domain from the rules, click the "Exclude" checkbox. Click the appropriate radio button to indicate if you are adding the application for inbound messages, outbound messages, or both.
From the table, select one or more rules to apply by clicking the "Enable" checkbox. At the bottom of the screen, select a default action to be taken for this user, group or domain. Click "Submit" to enter the new application.
Apply To:
Domain
Select User Group
Select Domain Group
Data:
thatdomain.com
Exclude:
Direction:
Inbound
Outbound
Both
ID
Name
System Defined
Enable
1
Test rule
2
Another rule
3
Process Rule
Default Action:
Pass Through
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status:
17

Blocking Unknown File Types

The Content Filtering Queue does not automatically support blocking of unknown file types in attachment filtering. However, because the filtering engine identifies as .unk those files whose extension is unknown, Administrators can add a rule in the Attachment Filtering Rule window to block attachments with the .unk extension. In this way, content filtering blocks attachments with unknown file types.

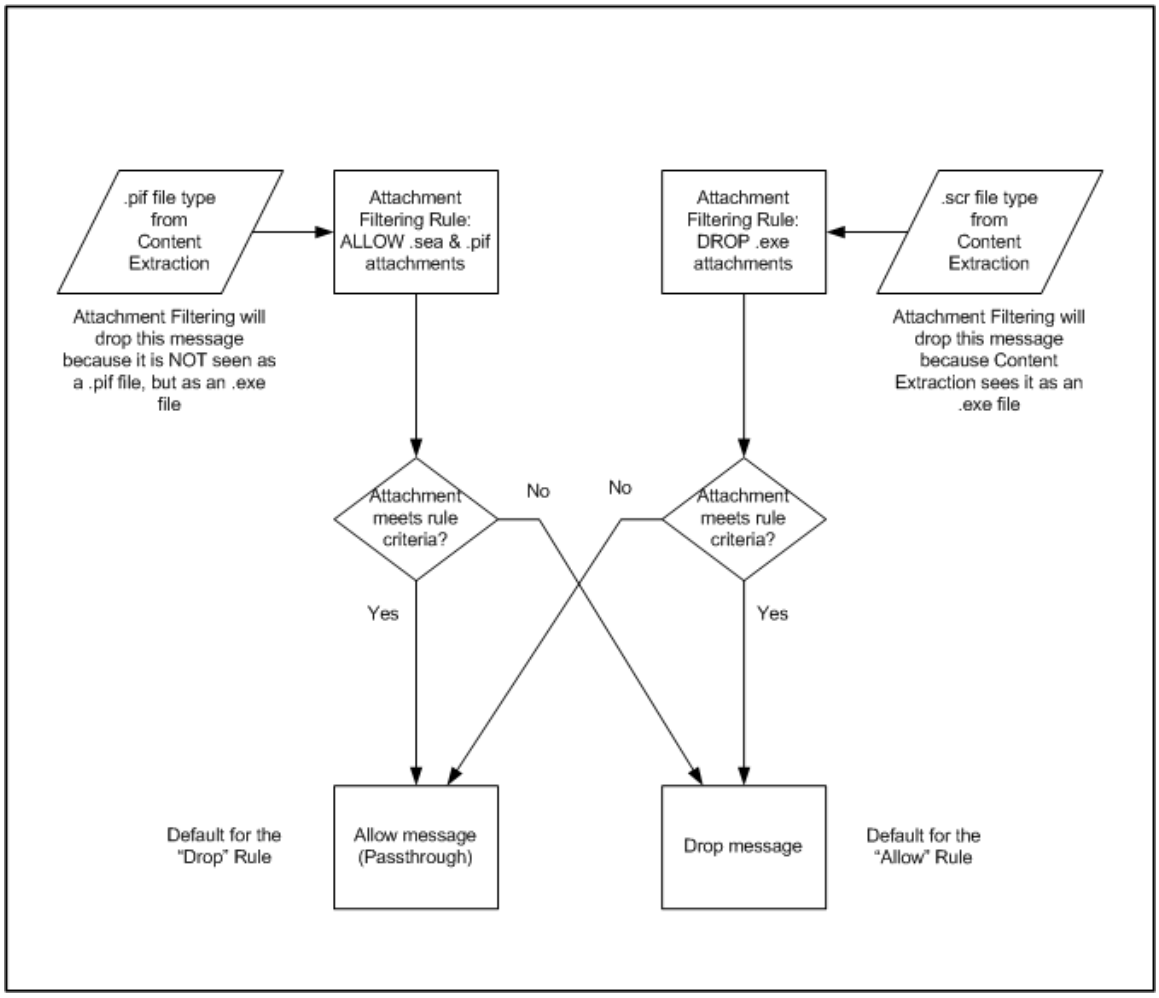
When filtering attachments, IronMail reads the file name extension and compares it with a bypass list. If the file type is present on the list, the attachment is treated according to filtering rules for the extension. If the extension is not in the bypass list, the attachment is treated as an unknown and an action is taken if a rule was set up for the .unk extension.

Remember that implementation of Attachment Filtering policies is a two-step process. First, Attachment Filtering "rules" must be created specify each file type and an IronMail response to each type. Second, the Attachment Filtering rules must be applied to users or groups or users—thereby creating Attachment Filtering "policies."

Attachment Filtering and Content Extraction

Special care must be taken when you create and apply rules that involve specific extension types. The extensions that are impacted are any extension — such as .scr, .pif, etc. — that is a specialized type of executable file. Content Extraction will normally interpret these files as .exe files.

The impact of this interpretation on Attachment Filtering is shown in the diagram below.


.pif file type from Content Extraction
Attachment Filtering Rule: ALLOW .sea & .pif attachments
Attachment Filtering Rule: DROP .exe attachments
.scr file type from Content Extraction
Attachment Filtering will drop this message because it is NOT seen as a .pif file, but as an .exe file
Attachment Filtering will drop this message because Content Extraction sees it as an .exe file
Attachment meets rule criteria?
No
No
Attachment meets rule criteria?
Yes
Yes
Default for the "Drop" Rule
Allow message (Passthrough)
Drop message
Default for the "Allow" Rule

The diagram above is based on the assumption that the Administrator wants to allow .pif and .sea files, but wants to stop .exe files. You can configure this intention either of two ways:

- by establishing an "Allow" *rule* that is intended to pass attachments with the specific extensions; or,
- by establishing a "Drop" rule that blocks all .exe attachments.

If either of these rules is configured exactly as shown in the diagram, neither will meet the intent of the Administrator. Both rules will drop the "allowable" attachments because CEQ interprets them all as .exe files in either case.

It is possible to configure specific rules that will capture or allow these extension types as the Administrator may desire. This is accomplished in the way the extensions are defined under the Attachment Filtering Rule Management screen.

Dangerous Extensions

The following extensions are capable of executing code on machines: att, bat, chm, cmd, com, cpl, eml, exe, hta, htm, html, ins, isp, js, jse, lnk, mp3, msi, msp,mst, pif, req, scr, sct, sct, shs, vbe, vbs, wav, wsc, wsf, wsh. Only add these extensions after they have been carefully reviewed to ensure that they are not used legitimately within the environment.

Default Replacement Text

An example of a Default Replacement Text message is: “This message was auto-generated by IronMail, the email security appliance protecting the ABC Corporation’s email infrastructure. In its concern for *network* security, ABC restricts certain file attachments from entering the network through email. This notice is being sent to you, notifying you that a file originally attached to this email was deleted.”

Filtering Message Content

Content Filtering

IronMail allows administrators to create policies based on keywords or phrases within email and their attachments. Content Filtering can be used as a tool to block spam, as well as to enforce acceptable email usage. IronMail is able to enforce Content Filtering policies for email messages, as well as over 20 text file attachment formats, including Microsoft Word, Novel WordPerfect for Macintosh, Lotus Word Pro, and Adobe Maker Interchange Format. (Note that while IronMail can scan for dictionary words and phrases within these documents, it does not scan the contents of "document properties"—such as the Microsoft Word properties *document author*, *document summary*, etc.)

The processing order within the Content Filtering feature is shown below:

Content Filtering				
	Content Filtering *Policy*	**Attachment Filtering Policy**	**Message Stamping Policy**	
From Previous Queue	Re-Route - do not proceed to next policy Drop Message - do not proceed to next policy Quarantine - proceed to next policy Secure Delivery - proceed to next policy Forward as Attachment - proceed to next policy Drop Part - proceed to next policy Replace - proceed to next policy Prefix - proceed to next policy Copy as Attachment - proceed to next policy	Re-Route - do not proceed to next policy Drop Message - do not proceed to next policy Quarantine - proceed to next policy Secure Delivery - proceed to next policy Forward as Attachment - proceed to next policy Drop Part - proceed to next policy Subject Re-write - proceed to next policy Copy as Attachment - proceed to next policy Copy - proceed to next policy	Stamp Messages - proceed to next policy	To Next Queue

	Copy - proceed to next policy Log - proceed to next policy	Rename - proceed to next policy Log - proceed to next policy Pass-Through - proceed to next policy		

Creating Content Filtering policies requires three steps:

1. Create “dictionaries” containing words or phrases that are disallowed.
2. Create “rules” based on dictionary “thresholds” that indicate that multiple dictionary words were detected in a message.
3. Create "policies" in which rules are applied to users and groups.

Whenever a message conforms to multiple rules, more than one action may be performed on that message. In some situations, not all actions can be performed.

- Policy attribute comparison is used to resolve conflicting actions. In the comparison, a system-defined policy supercedes a user-defined policy, a policy applied to a user supercedes a policy applied to a group, and a higher action code supercedes a lower one.
- If both secure delivery and forward actions could apply to a message, secure delivery has precedence because the forward action could cause the original message to be deleted and the message will not be securely delivered. Other actions can be applied along with secure delivery.
- Policy attribute comparison is performed to resolve the conflict above when the actions belong to different policies; just action codes are compared when both rules belong to the same policy.
- When multiple quarantine rules with finite quarantine days may be applied, policy attribute comparison is used to choose one of them. In this case, the quarantine period is compared instead of the action code.
- Policy attribute comparison is used to resolve the conflicts that will arise when drop part and replace/prefix actions are defined on the same dictionary. These are part level actions, and only one may be performed. The same is true if the actions are replace and prefix.
- Policy attribute comparison is used to resolve the conflicts that will arise from defining two replace/prefix actions replace/prefix actions are defined on the same dictionary. The part can be replaced or prefixed with either one of the action data values.
- Policy attribute comparison is used between two rules when one of them is a reroute, a drop *rule*, or a quarantine forever, and the other rule is an action in (4) or (5). A copy action in a policy applied to a user supercedes a reroute action applied to a group.
- Policy attribute comparison is performed between two rules when either of them is one of the following:
    - Reroute rule applied to a sender or subject,
    - Drop rule applied to a sender or subject, or
    - Quarantine forever.
- If one of the actions is a reroute or drop rule applied to a sender or subject or a quarantine forever, the one action will be performed and all other actions will be ignored because the message will no longer be available for additional actions.

Before implementing Content Filtering policies, careful attention must be paid to the dictionary entries and their weights. Careless use of dictionary words, weights, and thresholds can lead to IronMail taking action on otherwise legitimate email. For example, the presence of "breast" in a PORN dictionary might act on a message describing a chicken breast served at a meal, or a newsletter about breast cancer awareness month. Likewise users within the company may have the personal names "Lust," "Dick," "Beaver," or "Lolita"—words that might be present in a PORN dictionary. See the discussion of "best practices" using IronMail's Content Filtering policies.

IronMail ships with five dictionaries by default: **Porn**, **Confidential**, **Spam**, **Malicious Mobile Code, and URL**. The **Porn** dictionary contains hundreds of words that many would consider "adult" or inappropriate. The **Confidential** dictionary contains words and phrases that might suggest the secret sharing of information. The **Spam** dictionary contains hundreds of words and phrases commonly used by spammers. And the **Malicious Mobile Code** dictionary contains hundreds of keywords and commands used by scripting languages, such as JavaScript, ActiveX, C+, etc. The **URL** dictionary contains thousands of URLs known to be used by spammers. Administrators may create as many other dictionaries as their needs require.

Content Filtering is processed within the Content Filtering feature in SuperQueue. Accordingly, Content Filtering must be enabled and running in order for IronMail to enforce Content Filtering policies.

Multi-Part MIME Messages

When a message body contains both text and HTML, both the text and HTML are searched. Also, the HTML tags are removed and the remaining text is processed. This tag removal can result in a word combination that matches an IronMail search pattern, even though these words may not exist in the actual HTML version. For this reason, the Replace action is never attempted for this type of message.

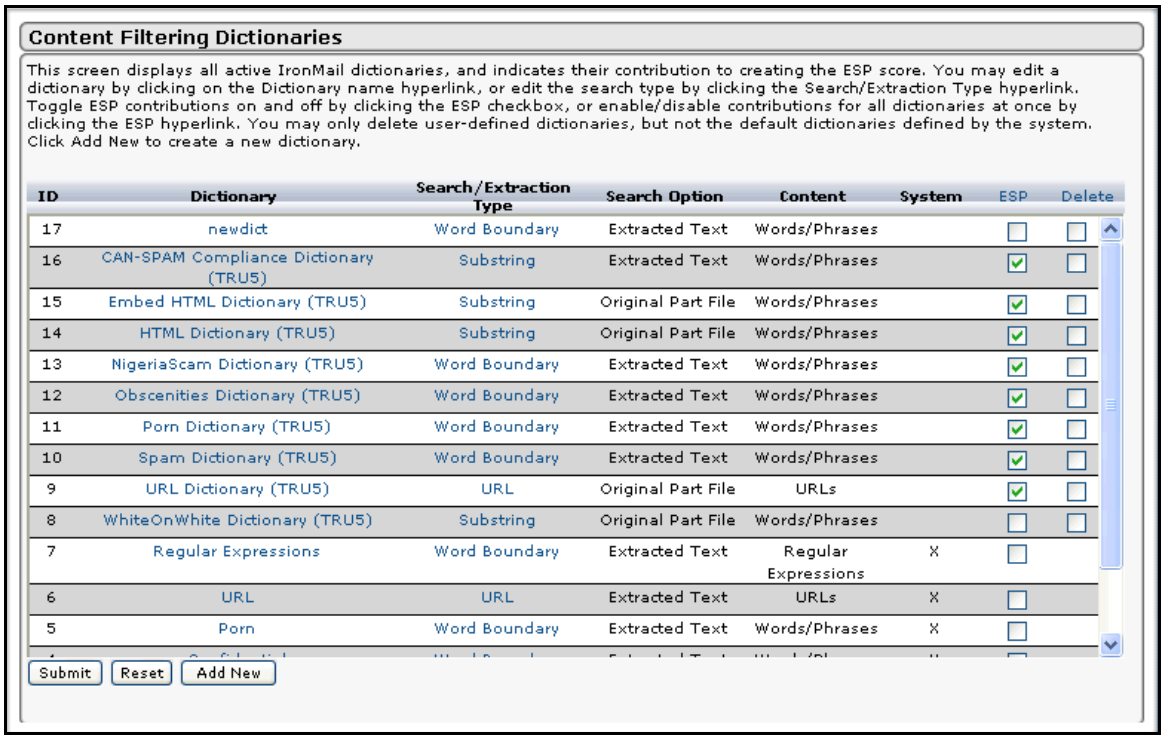
Note: Administrators may set a limit on how much of a message the Content Filtering engine will examine. In order to prevent the Content Filtering Queue from bogging down trying to examine very large messages, administrators may specify (in kilobytes) when to stop scanning a message. If the limit is set to 100 KB, IronMail will scan the first 100K of a message, and if it hasn't found a word in the dictionary by that point, it is assumed the remainder of the message is acceptable and scanning stops. Set the search limit at *Queue Manager > Configure Queues > SuperQueue > "Search Limit."*

The Content Filtering hyperlink in the left navigation frame expands to reveal Dictionaries, Manage Rules, and Apply Rules sub-menus.

Dictionaries

The Content Filtering Dictionaries page is where dictionaries are created and edited. In addition to the default system-generated dictionaries - **Porn**, **Spam**, **Confidentiality**, **Malicious Mobile Code and URL** - administrators can create their own dictionaries to enforce policies and fight spam. Search Types permit a search of email looking for dictionary words anywhere within a message when embedded within another word or text string, or search for words bounded by white space or other characters. In addition, the Search Option feature offers a choice of content filtering on raw email messages (for filtering on URLs or filtering against the "Malicious Mobile Code" Dictionary) or content filtering on extracted email text ignoring tags that spammers routinely use to hide content from spam detection software in both raw email messages and the extracted text.

The original (default) entries in the system-generated dictionaries should not be deleted. In most cases, the option to delete them will not exist. However, entries in the URL Dictionary currently offer the Delete option. ***The default entries should not be deleted.*** The same recommendation will apply to any other default entries in system-generated dictionaries. Users should only delete entries they have added, not defaults.

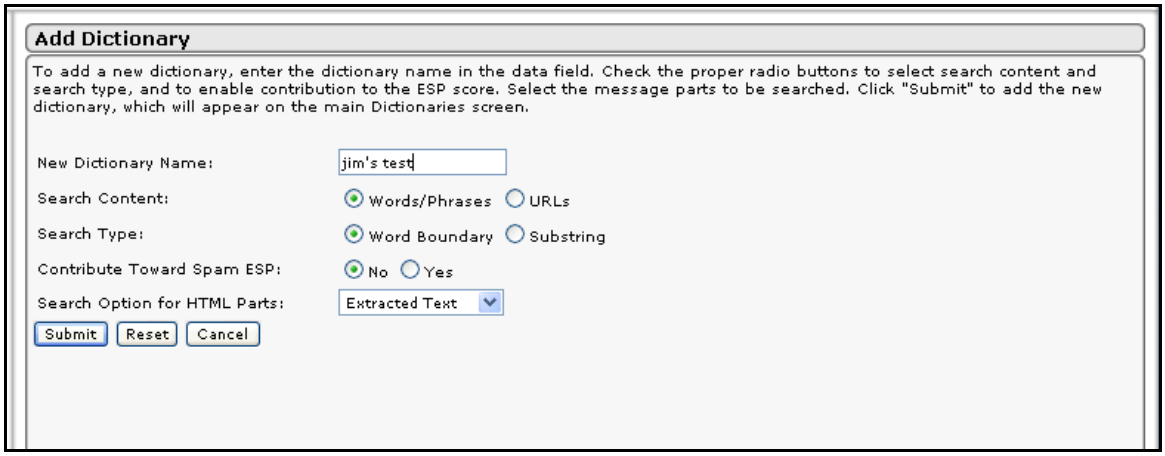

Content Filtering Dictionaries
This screen displays all active IronMail dictionaries, and indicates their contribution to creating the ESP score. You may edit a dictionary by clicking on the Dictionary name hyperlink, or edit the search type by clicking the Search/Extraction Type hyperlink. Toggle ESP contributions on and off by clicking the ESP checkbox, or enable/disable contributions for all dictionaries at once by clicking the ESP hyperlink. You may only delete user-defined dictionaries, but not the default dictionaries defined by the system. Click Add New to create a new dictionary.
ID
Dictionary
Search/Extraction Type
Search Option
Content
System
ESP
Delete
17 newdict Word Boundary Extracted Text Words/Phrases
16 CAN-SPAM Compliance Dictionary (TRU5) Substring Extracted Text Words/Phrases
15 Embed HTML Dictionary (TRU5) Substring Original Part File Words/Phrases
14 HTML Dictionary (TRU5) Substring Original Part File Words/Phrases
13 NigeriaScam Dictionary (TRU5) Word Boundary Extracted Text Words/Phrases
12 Obscenities Dictionary (TRU5) Word Boundary Extracted Text Words/Phrases
11 Porn Dictionary (TRU5) Word Boundary Extracted Text Words/Phrases
10 Spam Dictionary (TRU5) Word Boundary Extracted Text Words/Phrases
9 URL Dictionary (TRU5) URL Original Part File URLs
8 WhiteOnWhite Dictionary (TRU5) Substring Original Part File Words/Phrases
7 Regular Expressions Word Boundary Extracted Text Regular Expressions X
6 URL URL Extracted Text URLs X
5 Porn Word Boundary Extracted Text Words/Phrases X
Submit
Reset
Add New

The table of dictionaries contains five dictionaries by default, and offers the following information about each dictionary:

ID	This column displays the unique ID number that IronMail generates for each dictionary. IronMail's logs and reports will report statistics about each *rule*. Whenever a *policy* is enforced, the report or log will provide information about the message, and the specific Content Filtering dictionary ID responsible for causing IronMail to act on the message. Dictionary ID numbers are serially incremented. If a dictionary is deleted, IronMail does not re-use its ID number.
Dictionary	This column reports the dictionaries' name. (When manually-generated dictionaries are created, the administrator is prompted to "name" it.) The dictionary name is also a hyperlink opening a secondary browser window in which the dictionary may be edited.
Search/Extraction Type	This column lists the dictionaries' method of searching for dictionary words. The **Substring Search** looks for dictionary words found anywhere including words embedded within another word or text string. The **Word Boundary** search type only looks for dictionary words when they are embedded by white space or *certain characters*, such as punctuation.
Search Option	This column lists the one of three types of search processing: search the "Original Part" file including any embedded tags or URLs, perform an "Extract Text" search of the file ignoring tags, or search with "Both" processes and use the method that has the most dictionary hits.
Content	This column shows the type of content to be searched by Content Filtering, as configured when dictionaries are added or edited. Options are: • Words/Phrases • URLs

System	A mark in this column indicates whether the dictionary is system-generated or not. (IronMail's five default **dictionaries - Porn**, **Spam**, **Confidentiality**, **Mobile Malicious Code and URL -** are system-generated.)
ESP	A mark in this column indicates whether or not the dictionary will contribute its scores to the ESP for use in building the ESP Profile.
Delete	Selecting the **Delete** check box for a dictionary and clicking **Submit**, deletes a dictionary from the table. The five default system-generated dictionaries may not be deleted.

Adding a New Dictionary


Add Dictionary
To add a new dictionary, enter the dictionary name in the data field. Check the proper radio buttons to select search content and search type, and to enable contribution to the ESP score. Select the message parts to be searched. Click "Submit" to add the new dictionary, which will appear on the main Dictionaries screen.
New Dictionary Name:
jim's test
Search Content:
Words/Phrases
URLs
Search Type:
Word Boundary
Substring
Contribute Toward Spam ESP:
No
Yes
Search Option for HTML Parts:
Extracted Text
Submit
Reset
Cancel

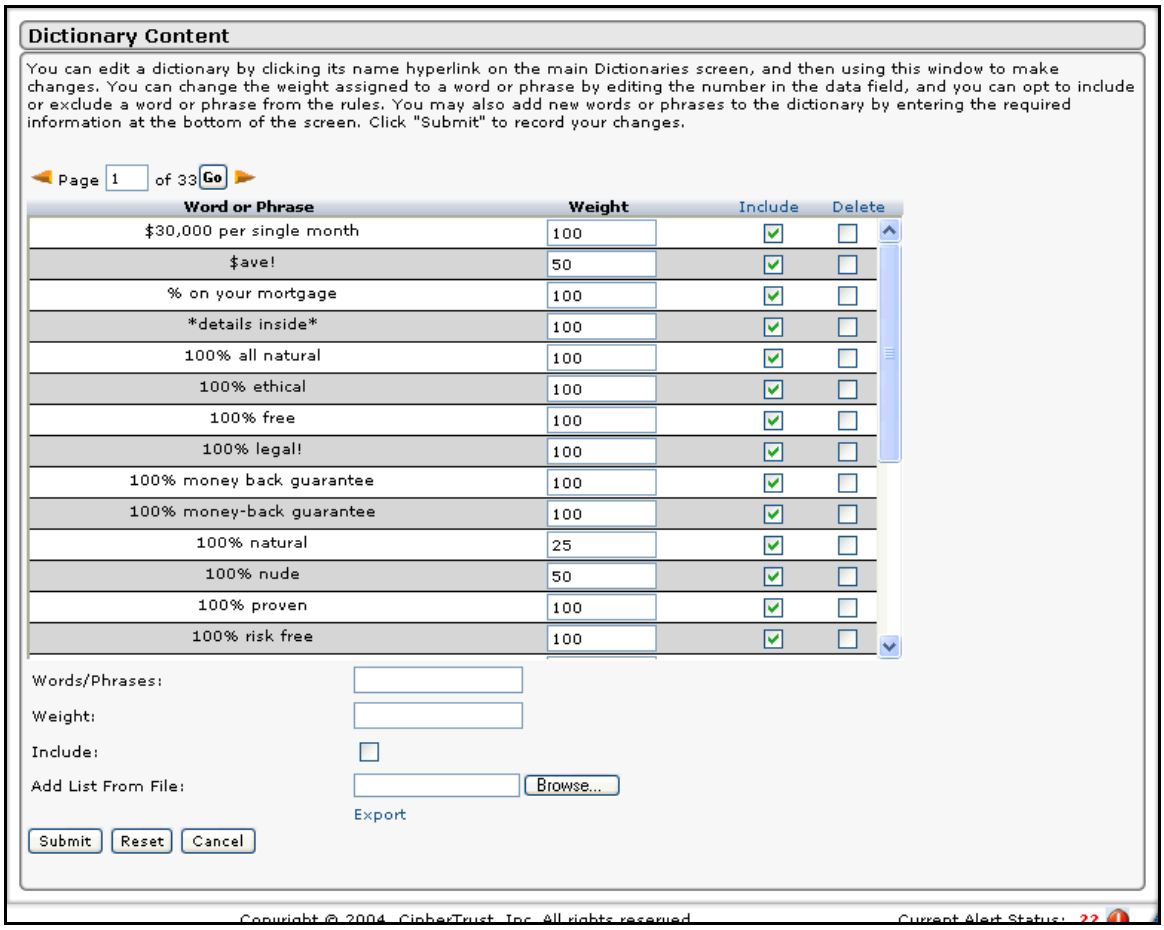
New Dictionary Name	Enter a dictionary name. The dictionary name will become a hyperlink opening a window in which the dictionary may be edited.
Search Content	Click the radio button to indicate the type of content to be searched by Content Filtering. Options are: • Words/Phrases • URLs
Search Type	Click the appropriate radio button to select the dictionay's method of searching for dictionary words. The **Substring Search** looks for dictionary words found anywhere, including words embedded within another word or text string. The **Word Boundary** search type only looks for dictionary words when they are bounded by white space or *certain characters*, such as punctuation.
Contribute Toward Spam ESP	Click the "Yes" radio button to have this dictionary contribute its score to be included in the ESP profile. Click "No" to have the dictionary act independently.
Search Option for HTML Parts	Select one of three types of search processing: search the "Original Part" file including any embedded tags or URLs, perform an "Extract Text" search of the file ignoring tags, or search with "Both" processes and use the method that has the most dictionary hits.

Click **Submit** to save the user input. The new dictionary is added to the table of dictionaries.

Important: Any dictionary must be *explicitly configured* to be used either in Content Filtering or as a part of the Spam ESP score.

Editing an Existing Dictionary

The Administrator can add, delete or change the individual entries within a dictionary. Clicking the Dictionary name hyperlink in the Content Filtering Dictionaries screen opens the Dictionary Content window.


Dictionary Content
You can edit a dictionary by clicking its name hyperlink on the main Dictionaries screen, and then using this window to make changes. You can change the weight assigned to a word or phrase by editing the number in the data field, and you can opt to include or exclude a word or phrase from the rules. You may also add new words or phrases to the dictionary by entering the required information at the bottom of the screen. Click "Submit" to record your changes.
Page 1 of 33 Go
Word or Phrase
Weight
Include
Delete
$30,000 per single month 100
$ave! 50
% on your mortgage 100
details inside 100
100% all natural 100
100% ethical 100
100% free 100
100% legal! 100
100% money back guarantee 100
100% money-back guarantee 100
100% natural 25
100% nude 50
100% proven 100
100% risk free 100
Words/Phrases:
Weight:
Include:
Add List From File:
Browse...
Export
Submit
Reset
Cancel
Copyright © 2004 CipherTrust, Inc. All rights reserved.
Current Alert Status:

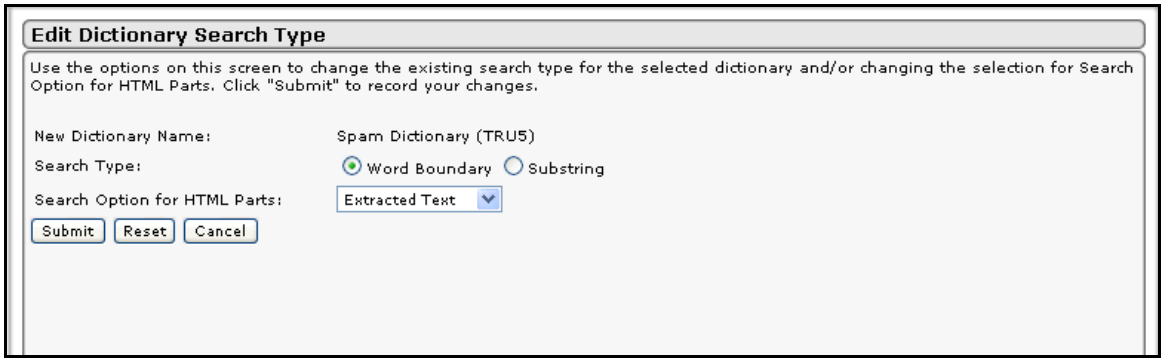
Field	Description
Navigation	If the contents of the dictionary is contained in multiple pages, a navigation option shows the current page being displayed and the total number of pages. Navigate one page at a time using the directional arrows, or go to a specific page by entering the page number in the Page data field.
Word or Phrase	This column lists the the specific words or phrases in the dictionary.
Weight	The weight for each word or phrase shows in this column. You may edit the weight by entering the new weight.
Include	An **Include** check box indicates if IronMail is configured to actively search for the specific word. If the box is not checked, the word or phrase will be ignored. Clicking the Enable hyperlink will toggle all entries on (to be included) or off (to be ignored).
Delete	Clicking the check box for a specific word or phrase will cause that entry to be deleted from the dictionary. Clicking the Delete hyperlink will cause ALL user-added entries to be deleted. **Note:** Do NOT delete default entries in system-generated dictionaries even if the option appears to exist.

New Entries	***The lower portion of the screen contains input fields to be used for adding new words or phrases.***
Word or Phrase	Enter a text string representing single or multiple words. The string may contain any printable character, and may be up to 256 characters long.
Weight	Enter a number in the **Weight** field. The "weight" is arbitrary, but should logically relate to the overall threshold when a Content Filtering rule is created. Negative weights may be entered by typing a hyphen before the number (e.g., "-125.") Use negatively-weighted words (representing keywords or phrases associated with legitimate business email) to offset the presence of positively-weighted dictionary words. IronMail subtracts the negative weights from the total score returned by Content Filtering. Medical institutions, for example, can create a variety of negatively-weighted medical terms to offset the presence of "breast" or "penis" whose presence might otherwise block legitimate messages.
Include	Select the **Include** check box to make IronMail actively search for the word or phrase when it examines a message. Note that dictionaries may contain words that are not "included." As administrators fine tune their dictionaries, they may toggle back and forth between including and excluding some words used in a Content Filtering policy.
Add lists from a file	If a list of keywords and phrases already exists in an ASCII text file, it may be imported using the **Browse** button. Browse to the text file and click **Submit**. The import file should contain one or more lines in the following format: `word_or_phrase|weight|include` *Where* **word_or_phrase** is a required field and represents the alphanumeric string to search for. *Where* **include** is a required field that accepts the following values: 0 = do not include 1 = include *Where* **weight** is a required field and represents the weight of the word or phrase.include). Some good examples of content filtering dictionary entries in an import file are: OFFICE XP|100|1 200 medications|100|1

Click **Submit** to save the user input. Enter new values in the input fields to continue building the dictionary.

Editing the Search Type

To modify the **Search/Extraction Type** for a dictionary, click its **Search/Extraction Type** hyperlink in the Content Filtering Dictionaries screen. The Edit Dictionary Search Type window opens.


Edit Dictionary Search Type
Use the options on this screen to change the existing search type for the selected dictionary and/or changing the selection for Search Option for HTML Parts. Click "Submit" to record your changes.
New Dictionary Name:
Spam Dictionary (TRU5)
Search Type:
Word Boundary
Substring
Search Option for HTML Parts:
Extracted Text
Submit
Reset
Cancel

Field	Description
New Dictionary Name	The name of the dictionary for which the Search Type is to be edited appears at the top of the screen. The name is not editable from this screen.
Search Type	The radio buttons indicate whether the dictionary is to be used to search Substrings or Word Boundaries. The current selection shows, and may be edited.
Search Option for HTML Parts	The current setting displays the search option for HTML searches. Options are: • Extracted Text • Original Part • Both You can edit this selection.

Click **Submit** to record changes.

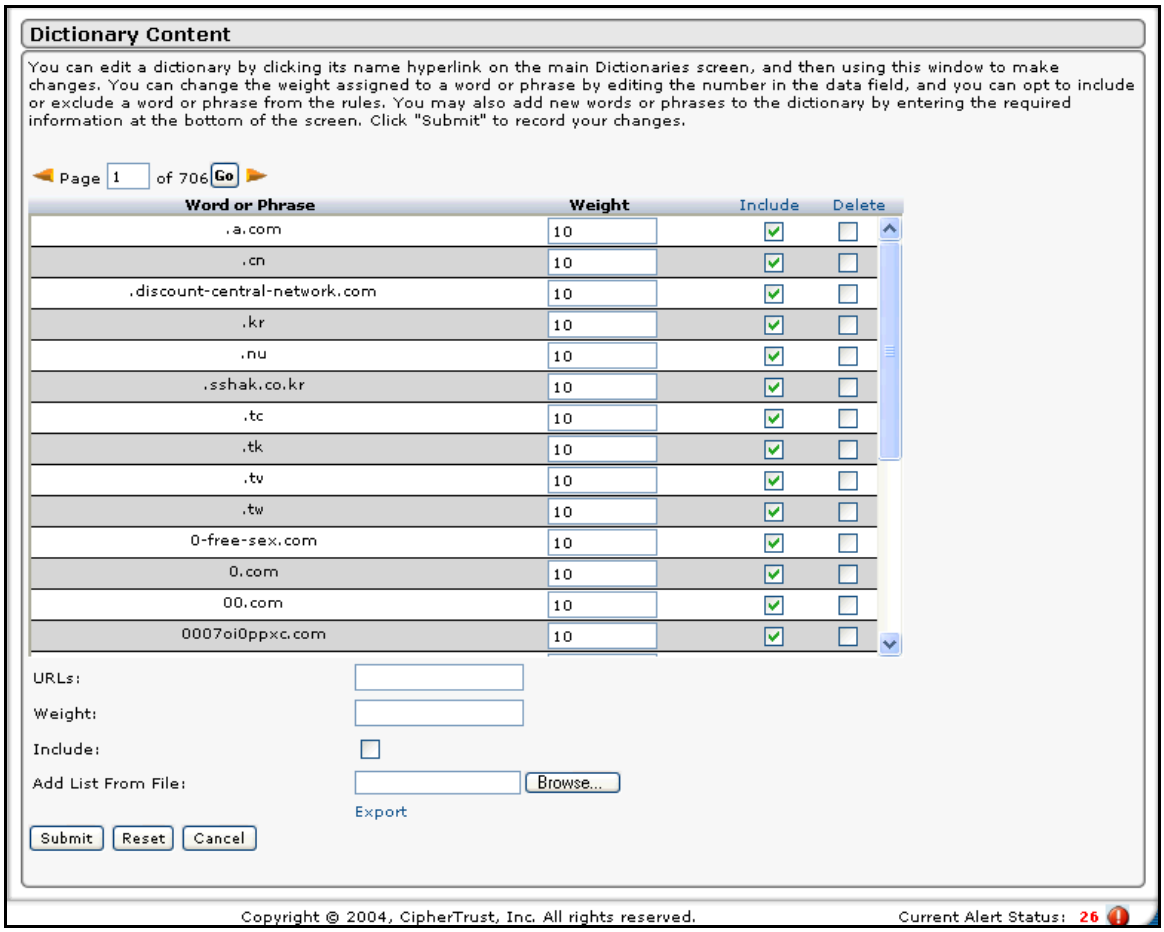
When the dictionaries have been reviewed and are ready to test, navigate to *Policy Manager > Content Filtering > Manage Rules* to create rules based on one or more of the dictionaries.

URL Filtering

URL Filtering functions as part of Content Filtering in IronMail. It exists as a dictionary that contains disallowed URLs. When Content Filtering scans an email message, it searches for URLs that match entries in the URL Dictionary and maintains a count of occurrences. If URL filtering is so configured, the resultant score becomes a part of Content Filtering's contribution to the Enterprise Spam Profiler (ESP) score, and is applied in the Spam Queue.

If Content Filtering is not configured to contribute to the ESP score, URL Filtering can result in action on its own if the score reaches a pre-configured threshold.

URL Dictionary content (shown below) displays like the content of any other dictionary, and may be edited in the same way.


Dictionary Content
You can edit a dictionary by clicking its name hyperlink on the main Dictionaries screen, and then using this window to make changes. You can change the weight assigned to a word or phrase by editing the number in the data field, and you can opt to include or exclude a word or phrase from the rules. You may also add new words or phrases to the dictionary by entering the required information at the bottom of the screen. Click "Submit" to record your changes.
Page 1 of 706 Go
Word or Phrase
Weight
Include
Delete
.a.com 10
.cn 10
.discount-central-network.com 10
.kr 10
.nu 10
.sshak.co.kr 10
.tc 10
.tk 10
.tv 10
.tw 10
0-free-sex.com 10
0.com 10
00.com 10
0007oi0ppxc.com 10
URLs:
Weight:
Include:
Add List From File:
Browse...
Export
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 26

The URL Dictionary is created from collected messages in CipherTrust's spam archive. The Content Filtering and Anti-Spam functions load the URLs as keys. The message is tokenized (stripped down to its 'root domain') by ignoring white spaces, comments, HTML tags, etc., and extracting the URLs. In applying its dictionaries. Content Filtering decides, based on the dictionary contents (words or URLs), whether to perform the "tokenization" routine or the "replace-it" routine.

If you use Content Filtering inside ESP, the URL Dictionary looks at the count and totals the hits for each URL (in the message part or attachments, per configuration). The results are returned as a raw score based on the count of times each URL appears. The score is calculated and sent to ESP to become part of Content Filtering's contribution if so configured.

If you use Content Filtering outside ESP, URL Filtering is applied within the Anti-Spam feature. The score from URL Filtering is treated the same way as scores from any of the dictionaries, contributing to actions Content Filtering takes on its own.

Note: CipherTrust provides regular updates to the URL Dictionary through the Threat Response Update process.

URL Decoding

Spammers attempt to avoid detection by spam-blocking tools by obscuring URLs with various encoding techniques. IronMail's URL Filtering is enhanced by the ability to decode specific types of encoded URLs so IronMail can detect the spam and/or the spammers. The following types of URLs can be decoded:

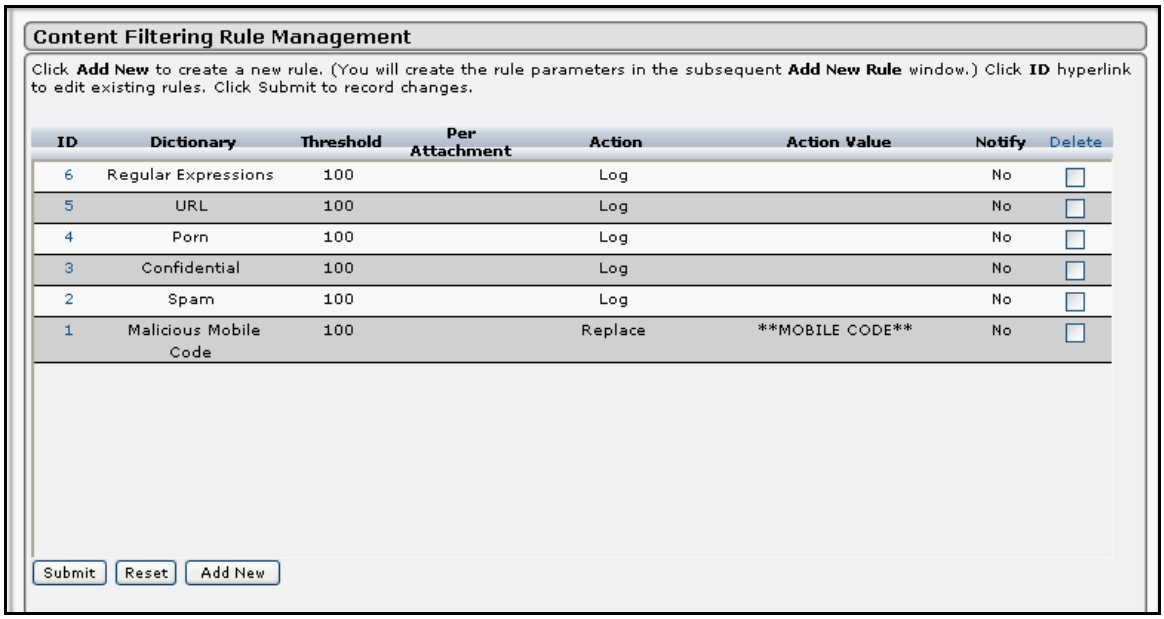
Encoding Type	Explanation
Hexadecimal string URLs	Spammers replace the letters in a URL with their equivalent hex code. When the user clicks on the link, the browser will decode the hex codes back to their original form. IronMail decodes the URL to see it in plain text, then finds it in the URL dictionary. **Example:** http://hotmail.com can be represented as: http://%77%77%77%2E%68%6F%74%6D%%61%69%6C%2E%63%6F%6D
Hexadecimal dotted IP URLs	Spammers encode the *IP address* in its hexadecimal form based on a calculation from the original IP address. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** the hexadecimal number for 207.178.42.40 is 0xCF.0xB2.0x2A.0x28, so http://207.178.42.40 can be represented as http://0xCF.0xB2.0x2A.0x28
Hexadecimal IP URLs	Spammers encode the IP address in its hexadecimal form as a non-dotted hex IP. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** http://207.178.42.40 can be represented as http://0xCFB22A28. It can be further obscured by adding an number of hexadecimal digits in front of the encoded URL, e.g., http://0x9AF0800CFB22A28
Decimal IP URLs	Spammers encode the IP address as a non-dotted decimal IP, based on a calculation from the original IP address. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** the calculated code for 206.159.40.2 is 3466536962, so http://206.159.40.2 can be represented as http://3466536962
Octal dotted IP URLs	Spammers represent the IP address in octal form, base 8. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** http://207.178.42.40 can be represented as: http://0317.0262.052.050, or http://000317.0000262.00052.0050
Character Entity Encoded URLs	Spammers use this method to represent characters in the HTML document in one of three ways: • as decimal numbers • as hexadecimal numbers • as names, in some cases. Only a few characters have names, but any character may be represented by a decimal number or hex number. IronMail supports decoding of decimal representations of character entities. **Example:** http://www.hotmail.com can be represented as: http://www.hotmail.com

IronMail does not decode Unicode-encoded URLs or mixed IP URLs.

This functionality must be enabled in Queue Manager > Configure Queues > Global Properties.

Manage Rules

The Content Filtering *Rule* Management page is where Content Filtering rules are made. (Rules are later converted into "policies" when they are applied to specific users or groups.)


Content Filtering Rule Management
Click Add New to create a new rule. (You will create the rule parameters in the subsequent Add New Rule window.) Click ID hyperlink to edit existing rules. Click Submit to record changes.
ID
Dictionary
Threshold
Per Attachment
Action
Action Value
Notify
Delete
6 Regular Expressions 100 Log No
5 URL 100 Log No
4 Porn 100 Log No
3 Confidential 100 Log No
2 Spam 100 Log No
1 Malicious Mobile Code 100 Replace **MOBILE CODE** No
Submit
Reset
Add New

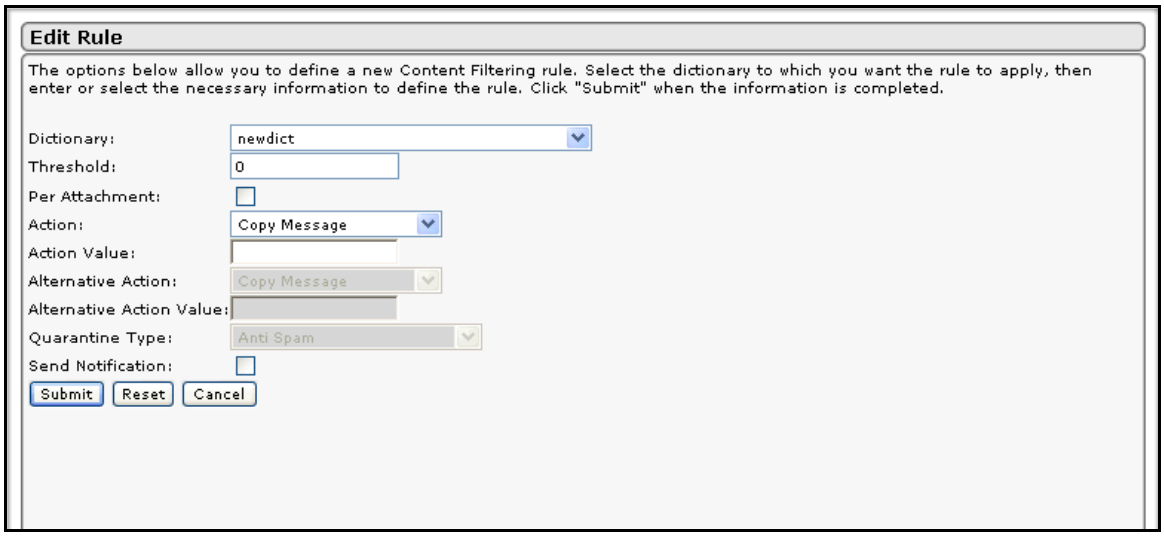
The table of rules, empty until one or more rules are created, displays the following information:

ID	This column displays the unique ID number that IronMail generates for each Content Filtering rule. Whenever a *policy* is enforced, IronMail's logs will provide information about the message, and the specific Content Filtering Rule ID responsible for causing IronMail to act on the message. Rule ID numbers are serially incremented. If a rule is deleted, IronMail does not re-use its ID number. The Rule ID is also a hyperlink opening a secondary browser window in which the rule may be edited.
Dictionary	This column displays the name of the dictionary used in a rule.
Threshold	This column reports the numeric threshold for the rule—the sum of individual dictionary word weights within a message after which an action will be taken.
Per Attachment	This column reports if the threshold applies to individual attachments. (If "Per Attachment" is not indicated, the threshold applies to the entire email…message body plus attachments.)
Action	This column reports the action IronMail will take if the rule's threshold is reached or exceeded.
Action Value	If the action requires qualifying information this column reports the additional action information. For example, a copy action requires a valid email address to which to copy the message, and a quarantine action requires a number representing how many days the message is to be quarantined.
Notify	This column indicates whether IronMail should send a brief email notification to a user that the message was acted upon by a Content Filtering policy.

Delete	A **Delete** check box allows administrators to delete rules from the table of Content Filtering rules. The Delete column heading is also a hyperlink. When clicked, the **Delete** check boxes for all rules in the table are selected or deselected.

Adding a Content Filtering Rule

Create a new rule by clicking **Add New**.



A secondary Add New Rule window opens, requesting the following information:

Dictionary	Select from the **Dictionary** pick list one of the dictionaries created in *Policy Manager > Content Filtering > Dictionaries*.
Threshold	Enter a number in this **Threshold** input field. (The number may be between 1 and 214,783,647) The number is arbitrary, but should relate to the weights of individual dictionary keywords and phrases. For example, if an organization has a "zero tolerance" policy for certain words, the word's weight and the rule's threshold should be identical. If a dictionary and rule are designed to filter certain types of messages where the presence of multiple words and phrases are the salient identifying feature, a threshold somewhat larger than the sum of several individual weights is required.
Per Attachment	Select the **Per Attachment** check box to force the threshold to be used only for each message part. That is, if any part of the email—message body or attachment—exceeds the threshold, take an action. This may be a useful way to account for messages that have been forwarded back and forth as attachments between individuals. For example, two dictionary words in an message body might not reach a rule's threshold. But if the threshold is applied to the entire message and the message is forwarded back and forth as attachments several times, the threshold might well be reached. Selecting this option allows relatively harmless messages to be delivered unchallenged.
Action	IronMail can perform one of 10 actions if a rule's threshold is reached or exceeded. Select an action from the **Action** pick list. Note that some actions require qualifying information to be entered in the **Action Value** field below. • **Secured Delivery:** IronMail will always deliver messages to or from the specified user, group, or domain securely. First, IronMail will attempt to deliver the message using S/*MIME*. If S/MIME is not supported, IronMail will see if PGP certificates have been installed, and attempt that secure method. If neither is available or

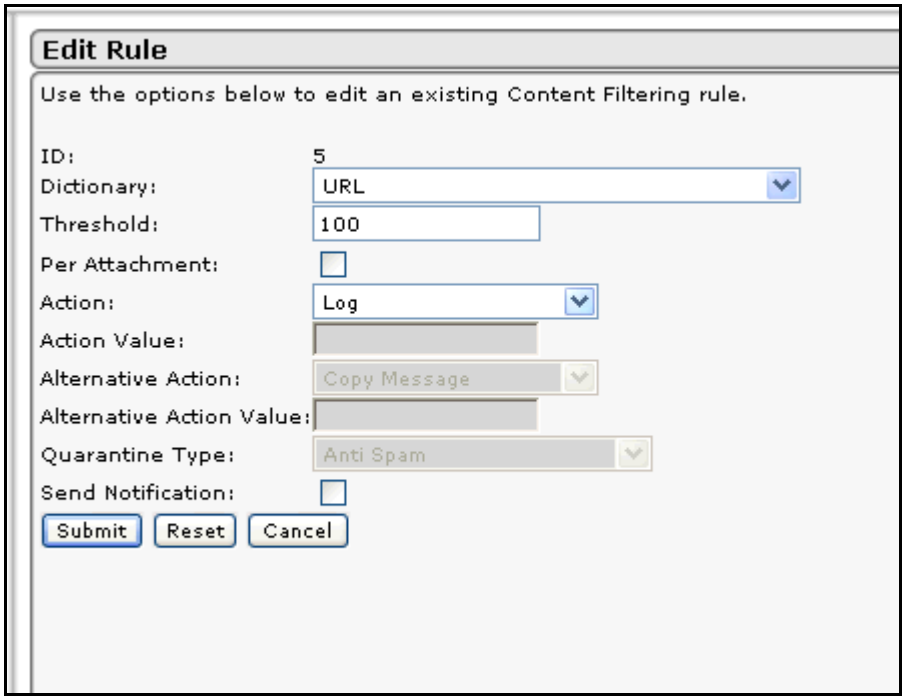
	unsupported by the other mail server, IronMail will attempt a *SSL* delivery. And if none of these can be supported, IronMail will deliver the message via HTTPS—its Secure Web Delivery. Select this option, for example, to encrypt messages that contain words indicative of sensitive or proprietary data. • **Log:** IronMail will deliver the message, but record in its Daily Policy Compliance Report that the message matched the conditions of the Content Filtering rule. (The Daily Policy Compliance Report is viewed in *Monitoring > Reports/Log Files > Reports*. Note that the "Daily Policy Compliance—Detailed" report must be manually enabled in *Monitoring > Reports/Log Files > Reports Configuration* in order for the log action to function • **Prefix:** IronMail will add a prefix to a found dictionary word an administrator-supplied text string. This may be useful, for example, when creating rules based on the Malicious Mobile Code dictionary. Potentially damaging computer-code words may be rendered ineffective until an administrator has had an opportunity to confirm whether the message is benign or not. Note that dictionary-word prefixing only functions if the word appears in the message body or plain text file attachments. IronMail cannot edit document attachments created by Microsoft Word or other 3rd party applications. Even though IronMail can *find* dictionary words in other file types, it cannot *edit* them. Consider implementing an alternate action for instances when this limitation applies. • **Re-route:** IronMail will re-route the message to a specified machine for additional processing. If the re-route action is specified, the *IP address* of the server must be entered in the **Action Value** input field below. • **Drop message:** IronMail will drop the entire message. Administrators may elect to send a brief IronMail-generated email, indicating that the message was dropped because of this Content Filtering rule. However, IronMail will only do so if **Send Notification** is enabled below, and also enabled in *Policy Manager > Content Filtering > Apply Rules*. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Value** field indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Value** field below. • **Drop part:** IronMail will drop just the file attachment. If a message is entered in the **Action Value** input field below, the message is appended to the email as a text file attachment. The message may state, for example, that files of the specified type are not allowed to enter the *network* via email attachments. If a message is not specified in the **Action Value** field, IronMail will replace the dropped part with a blank text file attachment. • **Replace:** IronMail will replace the found dictionary word with the text string provided in the **Action Value** input field below. Note that dictionary-word replacing only functions if the word appears in the message body or plain text file attachments. IronMail cannot edit document attachments created by Microsoft Word or other 3rd party applications. Even though IronMail can *find* dictionary words in other

	file types, it cannot *edit* them. Consider implementing an alternate action for instances when this limitation applies. **Note:** When a message contains both text and non-text types (such as html, doc, xls, etc.) the replace action will not be attempted in cases where text extraction results may result in different text and non-text versions of the message. In addition, because of the need to apply the same action on all parts of a message the replace action is not performed on many types of multi-part MIME messages. • **Copy as an attachment:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the **Action Value** column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Copy Message:** IronMail will deliver the original message but send a copy of the message to an alternate address. This action inserts the alternate address in the RFC821 Cc: header—it does not display in the RFC822 Cc: header.
Action Value	Some actions require qualifying information. • **Prefix:** this action requires a text string. The text string may be any printable character up to 256 characters long. For example, found dictionary words may be prefixed with the string "!!!!!!!" or "CHECK CODE!" • **Re-route:** this action requires a valid IP address of the host performing additional message processing. • **Quarantine:** this action requires a numeric value from 0 to 15. The number represents how many days the message will be quarantined before IronMail delivers it. For example, if a message is received at 12:30 PM on Wednesday and is quarantined for two days, IronMail will return the message to its regular mail flow at 12:30 PM Friday, and any queues that have not yet processed the message will do so before final delivery. A zero ("0") value, however, indicates "Do Not Deliver!" Any message with a quarantine value of zero will be automatically deleted according to the Cleanup Schedule for "Quarantine Data" (*System > Cleanup Schedule*). • **Forward Message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. (Do not insert spaces between commas and subsequent email addresses.) • **Drop part:** this action optionally requires a text string. The string may contain any printable character, and be up to 256 characters long. IronMail will replace the message part in which the dictionary threshold was reached with a plain text file attachment containing the text string provided here. If no text string is provided, IronMail will replace the message part with a blank text file attachment. • **Replace:** this action requires a text string and may contain any printable character, and be up to 256 characters long. • **Copy message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. (Do not insert spaces between commas and subsequent email addresses.)
Alternate Action	IronMail can only perform the prefix and replace actions on the email body, or in plain ASCII text files. It cannot edit Microsoft Word or Excel documents, for example. Therefore, if prefix or replace was selected as the action, indicate an alternate action if the first action cannot be performed. The list of alternate actions does not contain "prefix" or "replace."

Alternate Action Value	If the alternate action requires qualifying information, enter that alternate action value in this input field.
Quarantine Type	If the Quarantine action is selected in the **Action** pick list above, this **Quarantine Type** pick list becomes enabled. It displays the default quarantine queues, and any other queues that were manually created. Select a queue where messages detected by this Content Filtering rule will be sent.
Send Notification	An IronMail-generated email may be sent when a Content Filtering policy affects a message. The text of the notification is configured in *Policy Manager > Mail Notification*.

Editing a Content Filtering Rule

Edit a rule by clicking the rule ID hyperlink.



Field	Description
ID	The unique ID number for this rule appears at the top of the screen. It is not editable.
Dictionary	Select the dictionary to be used for this rule from the drop down list. The current selection shows.
Threshold	The current threshold for the rule shows in the data field. You may enter a new value.
Per Attachment	The current configuration is indicated by a mark in the checkbox. You may toggle this option on and off.
Action	The action to be taken by IronMail as a result of this rule shows in the data field. It can be changed by selecting another action.
Action Value	Any additional information required by a selected action is entered here, and should be changed to match the action if a new action is selected.

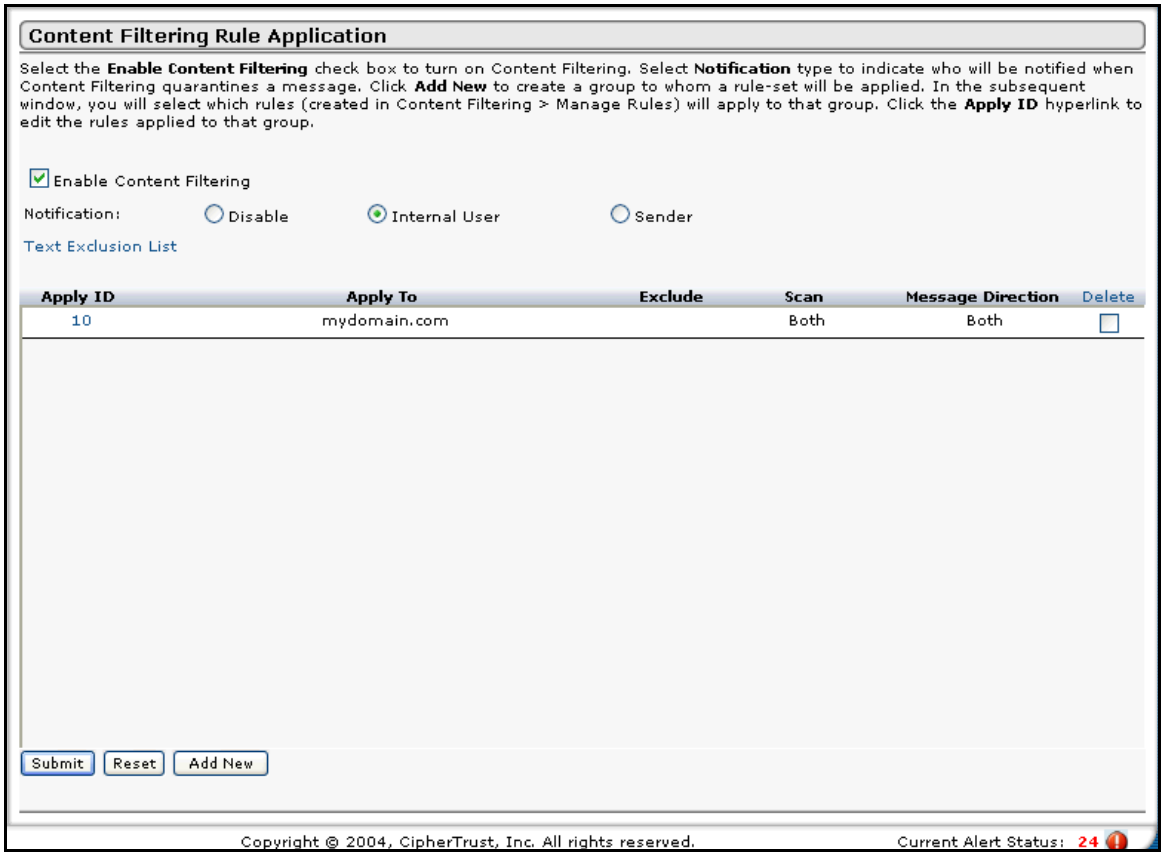
Alternative Action	Any alternate action to be taken when the primary action cannot be performed is selected from the pick list.
Alternative Action Value	Any additional information required by a selected action is entered here, and should be changed to match the action if a new action is selected.
Quarantine Type	If Quarantine is selected as an action, the quarantine type must be selected.
Send Notification	Clicking the checkbox enables or disables the sending of notice when the rule is triggered.

After editing the rule in the Edit Rule secondary window, click **Submit** to save the user input.

Content Filtering rules are not active until they are converted into "policies" by applying them to specific users or groups. Navigate to *Policy Manager > Content Filtering > Apply Rules* to create Content Filtering policies.

Apply Rules

Content Filtering rules are created in *Policy Manager > Content Filtering > Manage Rules*, but they do not become active until they are applied to specific users or groups. Only after the rules are converted into Content Filtering *policies* in this window will IronMail take the specified actions for messages processed by IronMail.


Content Filtering Rule Application
Select the Enable Content Filtering check box to turn on Content Filtering. Select Notification type to indicate who will be notified when Content Filtering quarantines a message. Click Add New to create a group to whom a rule-set will be applied. In the subsequent window, you will select which rules (created in Content Filtering > Manage Rules) will apply to that group. Click the Apply ID hyperlink to edit the rules applied to that group.
Enable Content Filtering
Notification:
Disable
Internal User
Sender
Text Exclusion List
Apply ID
Apply To
Exclude
Scan
Message Direction
Delete
10
mydomain.com
Both
Both
Submit
Reset
Add New
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 24

The screen contains the following information:

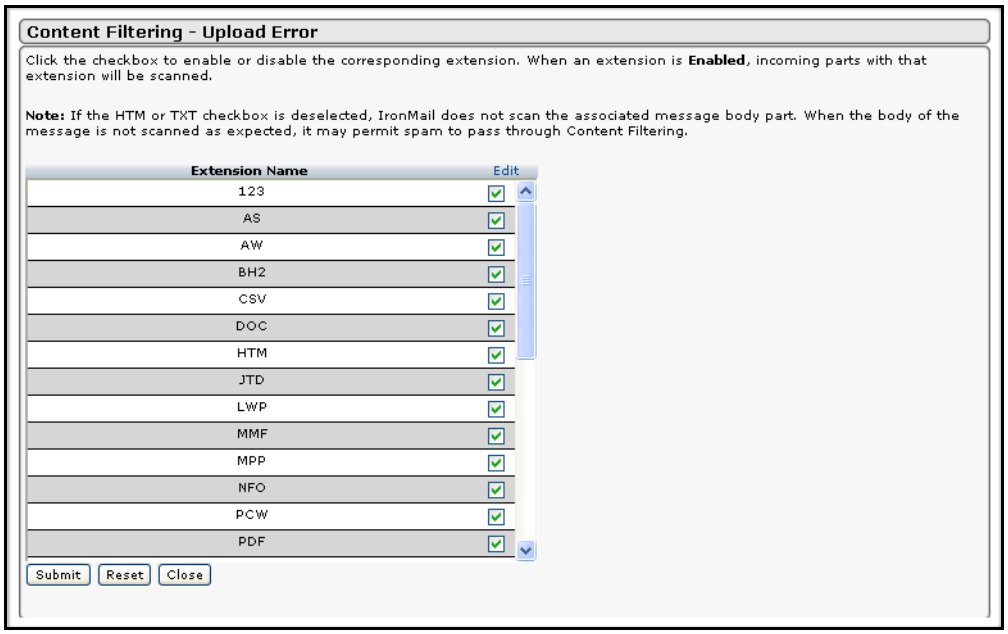
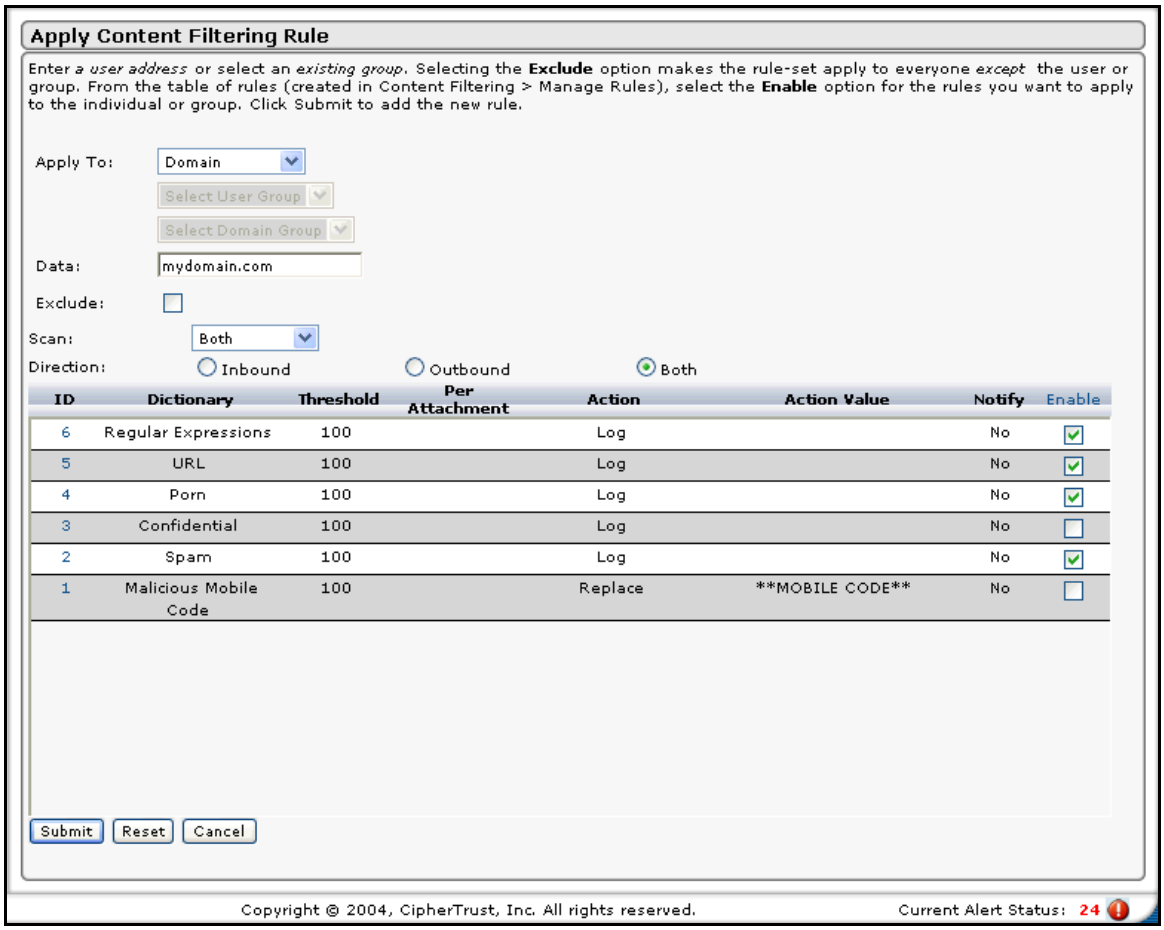
Field	Description
Enable Content Filtering	Select the **Enable Content Filtering** check box to enable, or "turn on," Content Filtering. If enabled, IronMail will enforce the Content Filtering policies listed in the table below. **Note:** Content Filtering policies are enforced, or processed, in the *Content Filtering Queue*, one of IronMail's queue subsystems. Therefore, the Content Filtering Queue must be set to Auto-Start, Running, and assigned a "queue position." The Web Administration user interface will allow **Enable Content Filtering** to be selected even if the Content Filtering Queue is not currently running, but the Content Filtering policies will not be enforced until the queue is enabled.
Notification	When Content Filtering rules were created in the *Policy Manager > Content Filtering > Manage Rules* page, an option provided for a notification to be generated if the *rule* acted upon a message. The notification setting here relates to that option. Three qualifying choices are available here: • Select **Disable** to override the notification setting within individual Content Filtering rules. If this radio button is selected, IronMail will not generate any notifications for any Content Filtering policy. • Select **Internal User** to send notifications only to users inside the *network*. Regardless of whether the internal user is the recipient or sender of the message, IronMail will generate a notification to him or her if a Content Filtering policy took an action on the message. • Select **Sender** to send notifications only to the message sender—the individual identified in the email's FROM address, regardless of whether he or she is inside or outside the network.
Text Exclusion List	Click the **Text Exclusion List** hyperlink to open a window displaying all text file-types IronMail is capable of scanning. Enable or disable file types as required. IronMail will examine all message parts with the specified extension (including file attachments) for the presence of dictionary words.  **Note:** If the HTM or TXT checkbox is deselected, IronMail does not scan the associated message body part. When the body of the message is not scanned as expected, it may permit spam to pass through Content Filtering.

Table of Rules	*The lower portion of the screen contains a list of all rules that are currently configured, and which may be applied.*
Apply ID	IronMail identifies each policy with a unique, serially incrementing ID number. Note that IronMail's serial numbers span all policies processed by the Content Filtering Queue. Thus, the ID numbers for Attachment Filtering, Content Filtering, and Message Stamping policies will not be duplicated—each time a policy within any of those three program areas is created, it is assigned the next higher number. IronMail's logs will report the policy ID number when messages meet the criteria of specific policies. The ID number is also a hyperlink that opens a secondary browser window in which the policy may be edited.
Apply To	This column reports the individual or group to whom the specific policy applies.
Exclude	A mark in the **Exclude** column indicates that the policy applies globally to everyone except the specified individual or group.
Scan	This column reports one of three values: Body, Attachment, or Both. • **Body:** IronMail will examine only the message body for the presence of dictionary words. • **Attachment:** IronMail will scan only file attachments for the presence of dictionary words. • **Both:** IronMail will scan both the message body and file attachments for the presence of dictionary words.
Message Direction	This column indicates the "direction" of mail for which the policy applies. One of three values will display: • **Inbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating outside the domain addressed to the user. If the specified user or group is outside the domain, then the policy is applied to all messages coming into the network from that user or group, regardless of the recipient address. • **Outbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating from those users and addressed to anyone outside the domain. If the specified user or group is outside the domain, then the policy is applied to all messages originating from within the network addressed to them, regardless of the senders' address. • **Both:** the policy affects all messages addressed to or received from the specified user or group.
Delete	To delete a policy, select its **Delete** check box and click **Submit**. Note that system-generated policies may not be deleted from this table. To delete a system-generated policy, navigate to *Policy Manager > Content Filtering > Manage Rules* and delete the specific rules that comprise the Content Filtering policy. Once all the rules are deleted, the policy will automatically be deleted from the table.

Adding a New Content Filtering Policy

Click **Add New** to generate a new policy based on specific rules created in *Policy Manager > Content Filtering > Manage Rules*. An Apply Content Filtering Rule secondary browser window opens.


Apply Content Filtering Rule
Enter a user address or select an existing group. Selecting the Exclude option makes the rule-set apply to everyone except the user or group. From the table of rules (created in Content Filtering > Manage Rules), select the Enable option for the rules you want to apply to the individual or group. Click Submit to add the new rule.
Apply To: Domain
Select User Group
Select Domain Group
Data: mydomain.com
Exclude:
Scan: Both
Direction: Inbound Outbound Both
ID Dictionary Threshold Per Attachment Action Action Value Notify Enable
6 Regular Expressions 100 Log No
5 URL 100 Log No
4 Porn 100 Log No
3 Confidential 100 Log No
2 Spam 100 Log No
1 Malicious Mobile Code 100 Replace **MOBILE CODE** No
Submit Reset Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 24

Provide the following input:

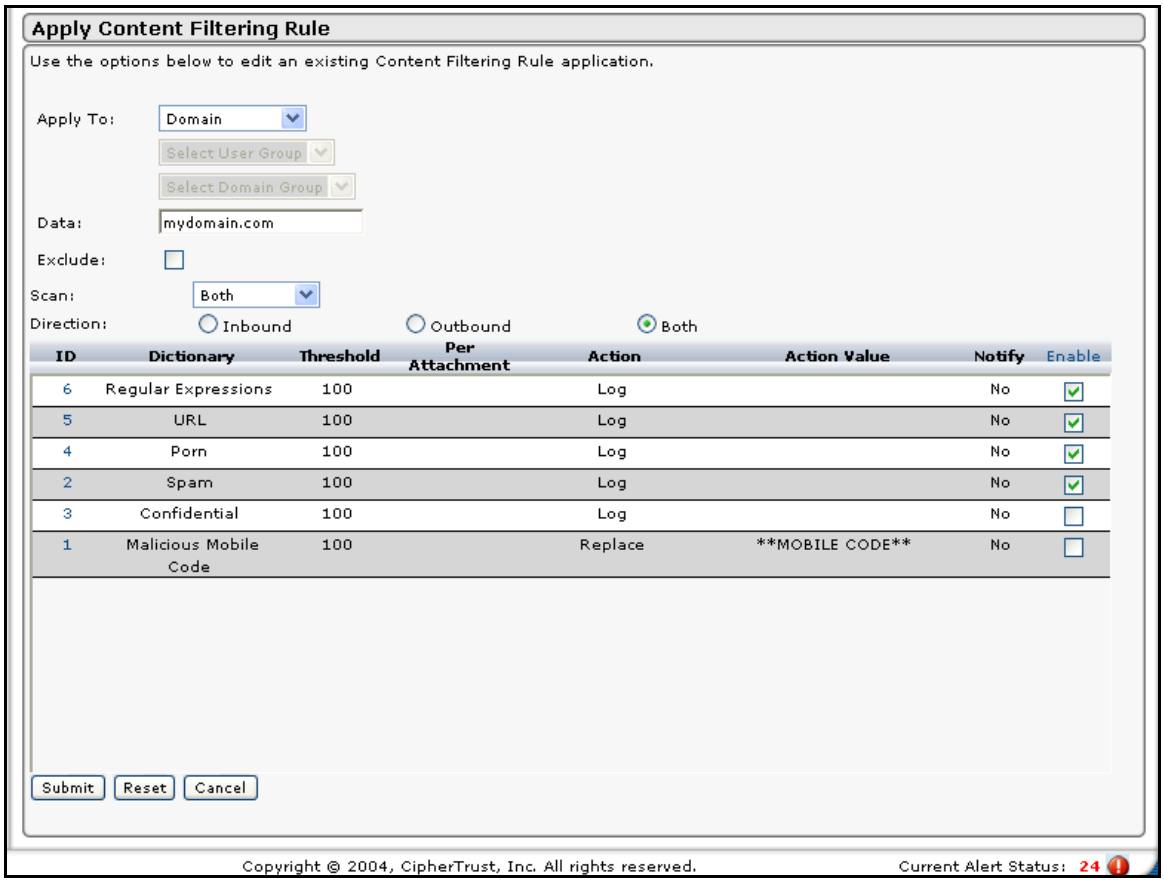
Apply To	Select the entity to which the rule is to be applied. Options are: • Email Address • Domain • User Group • Domain Group • Global
Data	To create a policy applying Attachment Filtering rules to a single individual, enter a valid email address in the **User** input field. (Multiple email addresses are not allowed in the **User** field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required.) To create a policy applying Attachment Filtering rules to a group of users, select the group name from the **Group** pick list. (All LDAP-imported groups as well as manually created groups are displayed in the pick list.) **Note:** a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. **Note:** the **Group** pick list contains the entry "Global." Select Global to apply the policy to everyone.

Exclude	Select the **Exclude** check box to apply the policy to everyone *except* the specified user or group. For example, if a rule states that messages with "adult content" words are to be quarantined, and this policy is applied to *Email Administrator* exclusively, then messages containing adult language will be quarantined for everyone except members of the *Email Administrator* group.
Scan	Select one of the options from the **Scan** pick list. This determines which part of a message IronMail should examine. • **Body:** IronMail will examine only the message body for the presence of dictionary words. • **Attachment:** IronMail will scan only file attachments for the presence of dictionary words. • **Both:** IronMail will scan both the message body and file attachments for the presence of dictionary words.
Direction	Specify the "direction" of mail for which the policy applies. • **Inbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating outside the domain addressed to the user. If the specified user or group is outside the domain, then the policy is applied to all messages coming into the network from that user or group, regardless of the recipient address. • **Outbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating from those users and addressed to *anyone* outside the domain. If the specified user or group is outside the domain, then the policy is applied to all messages originating from within the network addressed to them, regardless of the senders' address. • **Both:** the policy affects all messages addressed to or received from the specified user or group.
Table of Rules	***The lower portion of the screen contains a list of all rules that are currently configured, and which may be applied.***
ID	The unique IDs for all available rules are listed in this column.
Dictionary	In this column, the dictionary associated with the rule is displayed.
Threshold	The configured threshold for each rule shows in this column.
Per Attachment	If "Per Attachment" filtering has been enabled, an "X" in this column indicates that fact.
Action	The column the selected action for each rule.
Action Value	This column contains any required information associated with the configured action.
Notify	A "Yes" in this column indicates that IronMail is to send notices when this rule is triggered. If "No" appears, IronMail will not send notices.
Enable	Clicking this checkbox enables or disables the specific rule from the policy. Clicking the Enable hyperlink enables or disables all rules.

Click **Submit** to save the user input and create the policy. (The policy now displays in the Content Filtering Rule Application table in the Web Administration interface.) Click **Add New** again to create additional policies.

Editing an Existing Policy

Clicking the Apply ID in the Content Filtering Rule Application screen opens the same screen used for adding a new rule, with the exception that information about the rule in question is pre-populated. Edit the policy by changing the information.



Apply To	Select the entity to which the rule is to be applied. Options are: • Email Address • Domain • User Group • Domain Group • Global
Data	To create a policy applying Attachment Filtering rules to a single individual, enter a valid email address in the **User** input field. (Multiple email addresses are not allowed in the **User** field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required.) To create a policy applying Attachment Filtering rules to a group of users, select the group name from the **Group** pick list. (All LDAP-imported groups as well as manually created groups are displayed in the pick list.) **Note:** a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. **Note:** the **Group** pick list contains the entry "Global." Select Global to apply the policy to everyone.

Exclude	Select the **Exclude** check box to apply the policy to everyone *except* the specified user or group. For example, if a rule states that messages with "adult content" words are to be quarantined, and this policy is applied to *Email Administrator* exclusively, then messages containing adult language will be quarantined for everyone except members of the *Email Administrator* group.
Scan	Select one of the options from the **Scan** pick list. This determines which part of a message IronMail should examine. • **Body:** IronMail will examine only the message body for the presence of dictionary words. • **Attachment:** IronMail will scan only file attachments for the presence of dictionary words. • **Both:** IronMail will scan both the message body and file attachments for the presence of dictionary words.
Direction	Specify the "direction" of mail for which the policy applies. • **Inbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating outside the domain addressed to the user. If the specified user or group is outside the domain, then the policy is applied to all messages coming into the network from that user or group, regardless of the recipient address. • **Outbound:** If the specified user or group is inside the IronMail-hosted domain, then the policy is applied to all messages originating from those users and addressed to *anyone* outside the domain. If the specified user or group is outside the domain, then the policy is applied to all messages originating from within the network addressed to them, regardless of the senders' address. • **Both:** the policy affects all messages addressed to or received from the specified user or group.
Table of Rules	***The lower portion of the screen contains a list of all rules that are currently configured, and which may be applied.***
ID	The unique IDs for all available rules are listed in this column.
Dictionary	In this column, the dictionary associated with the rule is displayed.
Threshold	The configured threshold for each rule shows in this column.
Per Attachment	If "Per Attachment" filtering has been enabled, an "X" in this column indicates that fact.
Action	The column the selected action for each rule.
Action Value	This column contains any required information associated with the configured action.
Notify	A "Yes" in this column indicates that IronMail is to send notices when this rule is triggered. If "No" appears, IronMail will not send notices.
Enable	Clicking this checkbox enables or disables the specific rule from the policy. Clicking the Enable hyperlink enables or disables all rules.

Content Filtering and ESP

Content Filtering uses a slightly different approach to the ESP contribution than the Anti-Spam features. The value contributed to ESP is the same value that is returned to *Policy* Manager (in the event that CF is not configured to contribute to ESP). Each word that is matched during the CF process results in a point score based on the values in the specific dictionaries; the sum is the total point score for the message. The value can be relatively high, depending upon the message contents and individual word scores.

Values	Point score: individual word scores summed to generate a total point score. Threshold: a pre-configured value used by ESP in applying the Content Filtering contribution. Confidence value: a pre-configured percentage.
Formula	ESP Contribution = (Point Score/Threshold) X Confidence % In the formula, the threshold value acts as a ceiling limit for the point score so that no matter how high the raw point score may be, the value is capped at the threshold. The Point Score/Threshold cannot be over 100%.
Example 1: Point Score < Threshold	*If*: Each word has an individual score of 10 points; Threshold = 40; Confidence Value = 20%; and the words shown below match the Spam dictionary; *Then:* ID 0 Score 30 List ['entry,' 1 occurrence), ('guaranteed,' 1), ('take advantage,' 1)] Point Score = (1 x 10) + (1 x 10) + (1 x 10) = 30 points. ESP Contribution = (30/40) x 20% = 15 points
Example 2: Point Score > Threshold	*If*: Each word has an individual score of 10 points; Threshold = 40; Confidence Value = 20%; and the words shown below match the Spam dictionary; *Then:* ID 0 Score 50 List ['entry,' 1 occurrence), ('guaranteed,' 1), ('free,' 2),('take advantage,' 1)] Point Score = (1 x 10) + (1 x 10) + (2 x 10) (1 x 10) = 50 points. ESP Contribution = (50/40) x 20% = 20 points. This is due to the capped value.

If Content Filtering is configured to contribute to ESP, all enabled dictionaries will contribute. It is not possible to have Content Filtering enabled for ESP and still have any dictionary functioning independently.

Best Content Filtering Practices

Best Practice #1

Content Filtering policies should be manually reviewed for 1-2 weeks before they can be trusted to run unattended without fear of generating "false positives"—legitimate messages that the Content Filtering Queue thinks is spam or pornography. The preferred method for verifying the reliability of the *policy* is to make the policy's action "quarantine." When the Content Filtering policy quarantines a message, it sits in a temporary "storage area" where administrators may view its message header information as well as view the body (and attachments) of the email. A visual inspection of a message, and/or a look into IronMail's Content Filtering Queue Detailed Log will indicate whether the message is legitimate, and which dictionary words were responsible for sending it to the quarantine queue. In cases where the policy generated a "false positive," administrators will then edit the policy accordingly—either by removing the word from the dictionary, or changing the word's weight or the policy's threshold.

If more than one dictionary is used for Content Filtering policies, it is recommended that separate quarantine queues be created for each. (See *Queue Manager > Quarantine Types* for a discussion on creating multiple quarantine queues.) That is, create a "Content Filtering-PORN" queue to receive messages suspected of being pornography, and create a "Content Filtering-SPAM" queue to receive messages suspected of being spam. The use of separate queues for each dictionary simplifies management and review of Content Filtering policies.

Best Practice #2

Dictionaries should not contain words that, used in other contexts, are legitimate. For example, the word "hot" might appear in pornographic email, but it also appears in the context of weather, the temperature of coffee, etc. Single words are more likely to generate false positives than multiple-word strings. For example, "fresh lolita photos" and "extreme hardcore fetish" will be much more effective in stopping pornography than using any of the words individually. Consider reading samples of actual messages that a dictionary is intended to stop—extract word strings from those messages that will only appear in that genre of email.

Best Practice #3

Ensure that someone in the Human Resources department provides a clear statement of acceptable and unacceptable email usage. Where is the line drawn between acceptable "colorful" language and the use of expressly forbidden words? Is a single instance of the "f-word" cause for interdiction? Are other words allowed greater leniency? If a word is allowed once, why can't it appear ten times? Does it even make sense to add a word to a dictionary, assign it a weight, and create a *rule* that blocks the message if the word appears enough times to trigger a threshold? These are examples of conundrums with which administrators or HR personnel will have to wrestle.

Best Practice #4

In large mail volume environments (50,000+ messages a day), the size of IronMail's daily Content Filtering Queue Detailed Log file will quickly grow so large that it may not be practical to open it in a browser window within IronMail's graphical Web Administration user interface. Administrators are strongly encouraged to logon to IronMail's Command Line Interface through an SSH client while simultaneously logged onto the Web Administration interface. Administrators can view, in Web Administration's Quarantine Queue Message Header Details window, which messages need to be researched, and then switch to the Command Line Interface to immediately find the specific words and word counts that caused the message to be quarantined. While administrators can always view the message body from within the Message Detail window in order to identify the dictionary words that were detected, using the Command Line Interface is typically much more efficient.

Best Practice #5

While IronMail is a robust application capable of processing tens of thousands of messages per hour, the Content Filtering Queue is the one area of message-processing vulnerable to performance degradation. IronMail examines a message for dictionary matches once for each enabled dictionary. If twenty dictionaries are enabled, IronMail will examine the message twenty times before allowing it to move to the next queue in-line. If twenty 1,000-word dictionaries are enabled, message processing will obviously take longer than if five 200-word dictionaries are used. Therefore, in high mail-volume environments (50,000+ message per day), administrators are advised to be cautious when using multiple dictionaries.

There is no difference in IronMail performance if ten 1,000-word dictionaries are used, or five 2,000-word dictionaries are used. Neither is there a performance difference between "substring" or "word boundary" dictionaries.

Administrators may examine the Content Filtering Queue Detailed Log to see the time stamp when the Content Filtering Queue began examining a message and when it ended the examination. Checking the statistics for a variety of message sizes will provide an indication if IronMail performance may be affected with multiple and/or large dictionaries in place.

Note that Content Filtering Queue properties page allows the configuration of an upper limit on how much of a message the Content Filtering Queue examines. If a dictionary threshold has not been reached by this limit, it may be assumed that the message is not spam or pornography.

Stamping Messages

Message Stamping

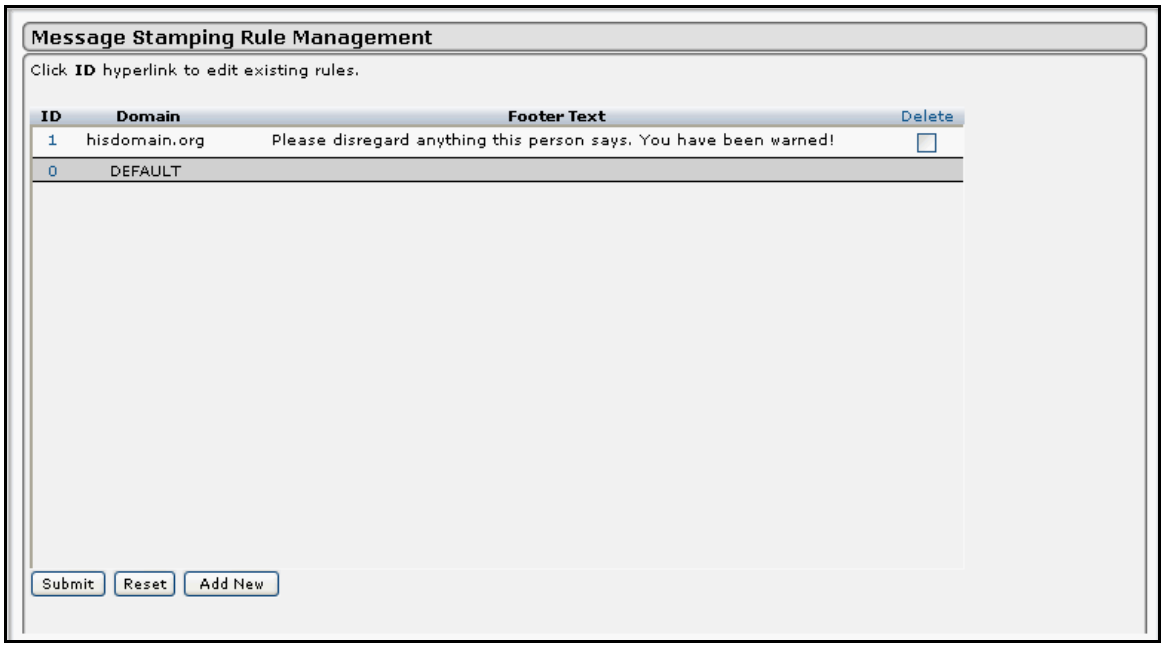
IronMail offers the ability to add “footer messages” at the end of outgoing messages sent in plain text format. Administrators may create various policies that are applied to individuals and groups for any of the domains IronMail hosts. Thus, all outgoing messages from members of the engineering group in XYZ domain (if hosted by IronMail) can be “stamped” with one message, while messages from the sales group at XYZ domain can be stamped with another message.

Message Stamping is processed in the *Content Filtering* feature. Accordingly, Content Filtering must be enabled and running in order for IronMail to enforce Message Stamping policies.

The Message Stamping hyperlink in the left navigation frame expands to offer Manage Rules and Apply Rules sub-menus.

Manage Rules

The Message Stamping *Rule* Management table contains one entry by default until additional Message Stamping rules are created. The word “DEFAULT” signifies the default domain that IronMail hosts (Administrators specified a default domain when running the Initial Configuration Wizard when IronMail was first installed). Thereafter, if IronMail hosts multiple domains, any one of them may be designated as the default in *Mail-Firewall > Mail Routing > Domain-based*. The default domain is the domain (i.e. the address) from which IronMail will send its notification alerts and Delivery Status Notifications.



The Rule Management table displays the following information:

ID	This column displays the unique ID number that IronMail generates for each Message Stamping rule. Whenever a *policy* is enforced, IronMail's reports or logs will provide information about the message, and the specific Message Stamping Rule ID that stamped a footer to a message. Rule ID numbers are serially incremented. If a rule is deleted, IronMail does not re-use its ID number. The Rule ID is also a hyperlink opening a secondary browser window in which the rule may be edited.
Domain	This column identifies the domain for which the rule applies. All messages originating from the specified domains will be stamped—conditional upon the users or groups for whom a Message Stamping policy is applied (see *Policy Manager > Message Stamping > Apply Rules*). IronMail only stamps outgoing messages from domains that it hosts.
Footer Text	This column displays the message that can be stamped on outgoing messages from the associated domain. (Multiple "rules" or messages can be created for a single domain—different rules can be applied to different users or groups within the domain.)
Delete	A **Delete** check box allows the deletion of a Message Stamping rule.

Note that once a message has been created for the default domain, it may not be deleted. The message text may be edited but not removed. To disable message stamping for the default domain, disable Message Stamping by deselecting the **Enable Message Stamping** check box in the Message Stamping Rule Application window.

Adding a New Rule

Clicking the Add New button at the bottom of the Message Stamping Rule Management screen opens the Add New Rule screen. Use this screen to create additional Message Stamping rules.

Add New Rule
Enter a domain name and a message to be stamped on email addressed from that domain.
Domain Name:
hisdomain.org
Please disregard anything this person says. You have been warned!
Footer Text:
Submit
Reset
Cancel

Field	Description
Domain Name	Enter a domain name in this field. This is the domain from which the stamped message will be sent. This must be a domain hosted by IronMail.
Footer Text	Enter the text for the stamped message, up to 1024 characters. This text will be appended to the bottom of the outgoing messages from the domain.

Click **Submit** to create the new rule and update the Message Stamping Rule Management screen.

Editing an Existing Rule

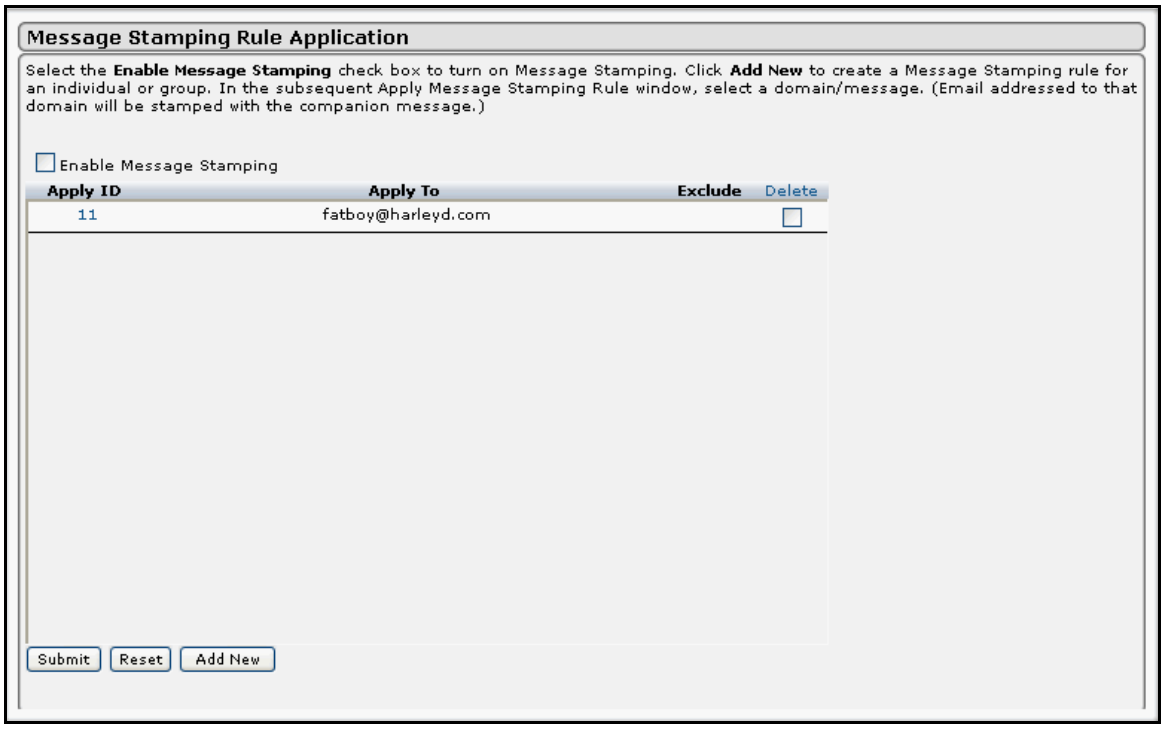
Clicking the ID hyperlink on the Message Stamping Rule Management screen opens the Edit Rule screen. Here you may alter the footer text and the domain name for any rule except Default.

Field	Description
Domain Name	Enter a domain name in this field. This is the domain from which the stamped message will be sent. This must be a domain hosted by IronMail.
Footer Text	Enter the text for the stamped message, up to 1024 characters. This text will be appended to the bottom of the outgoing messages from the domain.

Click **Submit** to record your changes.

Apply Rules

Message Stamping rules are created in *Policy Manager > Message Stamping > Manage Rules*, but they do not become active until they are applied to specific users or groups. Only after the rules are converted into Message Stamping policies in this window will IronMail write the specified footers to outgoing email.


Message Stamping Rule Application
Select the Enable Message Stamping check box to turn on Message Stamping. Click Add New to create a Message Stamping rule for an individual or group. In the subsequent Apply Message Stamping Rule window, select a domain/message. (Email addressed to that domain will be stamped with the companion message.)
Enable Message Stamping
Apply ID
Apply To
Exclude
Delete
11
fatboy@harleyd.com
Submit
Reset
Add New

Select the **Enable Message Stamping** check box to "turn on" IronMail's Message Stamping functionality.

Below the **Enable Message Stamping** option is the Message Stamping *Rule* Application table, empty until policies are created.

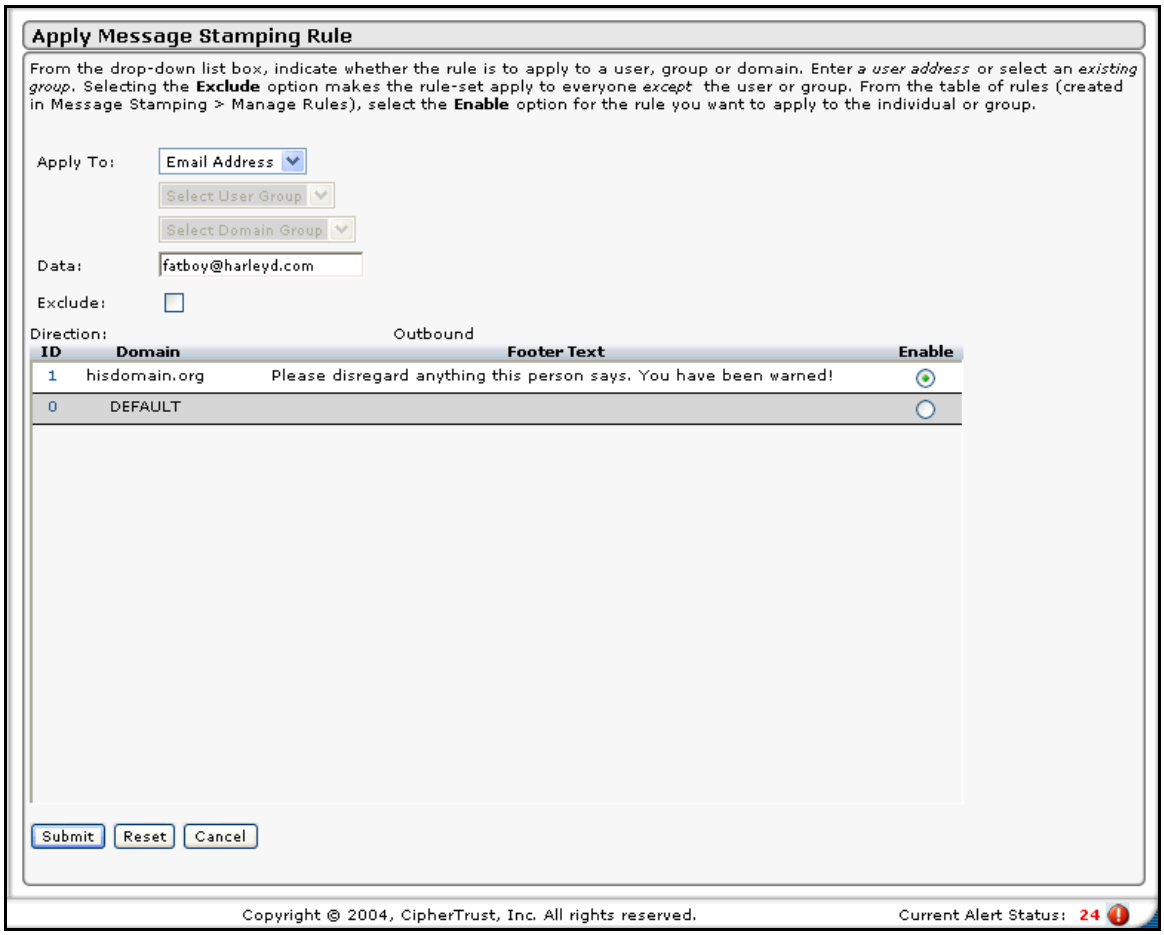
The table displays the following information:

Apply ID	IronMail identifies each policy with a unique, serially incrementing ID number. Note that IronMail's serial numbers span all policies processed by the Content Filtering Queue. Thus, the ID numbers for Attachment Filtering, Content Filtering, and Message Stamping policies will not be duplicated—each time a policy within any of those three program areas is created, it is assigned the next higher number. IronMail's logs and Daily Policy Compliance Reports will report the policy ID number when messages meet the criteria of specific policies. The ID number is also a hyperlink that opens a secondary browser window in which the policy may be edited.

Apply To	This column reports the individual or group to whom the specific policy applies.
Exclude	A mark in the Exclude column indicates that the policy applies globally to everyone except the specified individual or group.
Delete	Select a policy's **Delete** check box and click **Submit** to delete a policy from this table.

Adding a New Policy

Click **Add New** to create a Message Stamping policy. A secondary Message Stamping Rule window opens in which the policy parameters are entered.


Apply Message Stamping Rule
From the drop-down list box, indicate whether the rule is to apply to a user, group or domain. Enter a user address or select an existing group. Selecting the Exclude option makes the rule-set apply to everyone except the user or group. From the table of rules (created in Message Stamping > Manage Rules), select the Enable option for the rule you want to apply to the individual or group.
Apply To:
Email Address
Select User Group
Select Domain Group
Data:
fatboy@harleyd.com
Exclude:
Direction:
Outbound
ID
Domain
Footer Text
Enable
1
hisdomain.org
Please disregard anything this person says. You have been warned!
0
DEFAULT
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status:
24

The following input is requested in the secondary browser window:

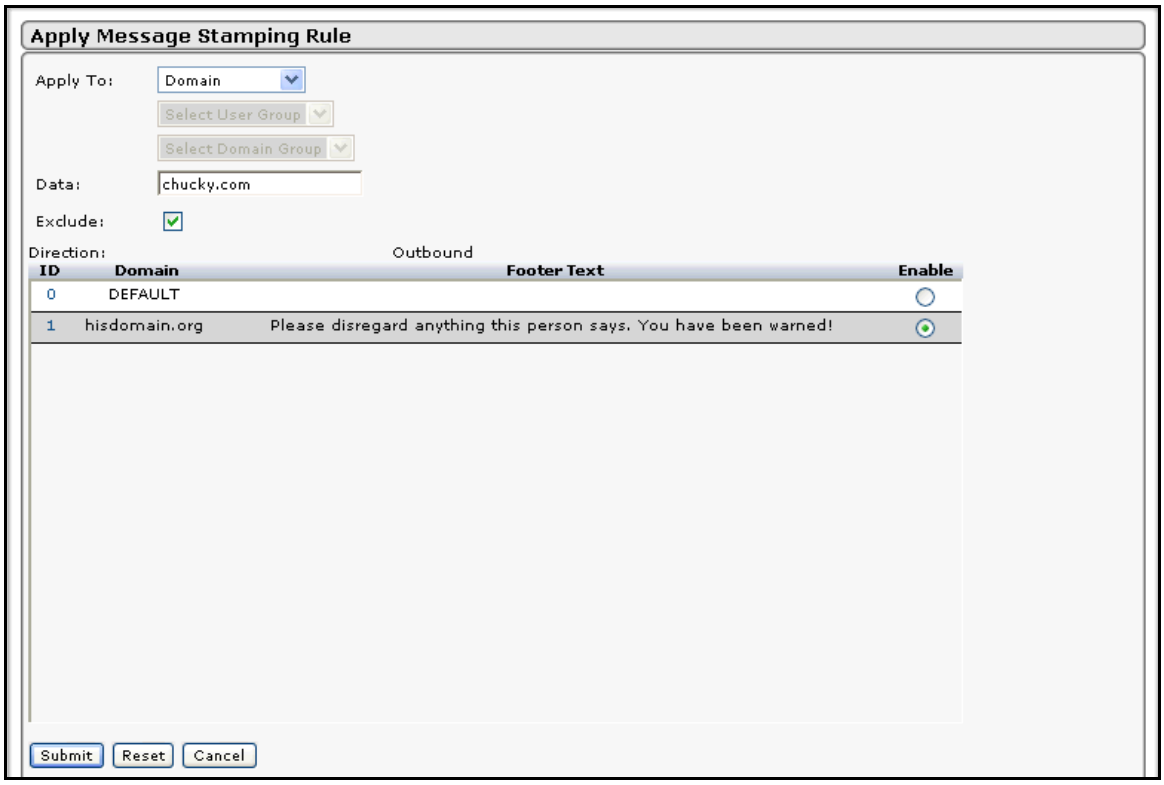
Field	Description
Apply To	Select the entity to which the rule will apply. • Email Address • Domain • User Group • Domain Group • Global

Data	To make a Message Stamping policy apply to a single individual, enter a valid email address in the User input field. (Multiple email addresses are not allowed in the **User** field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required.) To create a policy applying a Message Stamping rule to a group of users, select the group name from the **Group** pick list. (All LDAP-imported groups as well as manually created groups are displayed in the pick list.) Note that a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. Note that the **Group** pick list contains the entry "Global." Select Global to apply the policy to everyone.
Exclude	Select the **Exclude** check box to apply the policy to everyone except the specified user or group. For example, if a rule states that outgoing messages from domain.com are to be stamped, and this policy is applied to david.scott@domain.com exclusively, then messages from everyone in domain.com except david.scott will be stamped.
Direction	An **Outbound Message Direction** radio button is selected by default and cannot be changed. By definition, IronMail only stamps outbound messages that it delivers for the internal mail servers it hosts.
Table of Rules	***The lower portion of the screen lists all existing rules that may be applied.***
ID	This column contains the unique ID for each rule. The ID is also a hyperlink that allows the rule to be edited.
Domain	This column lists the domain to which each rule is applied.
Footer Text	The footer text for the specific rule displays in this column.
Enable	Clicking the radio button associated with a rule enables that rule for the policy being created. Each policy may have only one rule enabled.

Click **Submit** to save the user input and create the policy. The policy now displays in the Message Stamping Rule Application table. Click **Add New** again to create additional policies.

Editing an Existing Policy

Clicking the Apply ID hyperlink in the Message Stamping Rules Management screen opens the same screen used to add new rules (Apply Message Stamping Rule), with the only difference being that the configuration for the rule being edited is pre-populated. Make changes to the information on the screen.



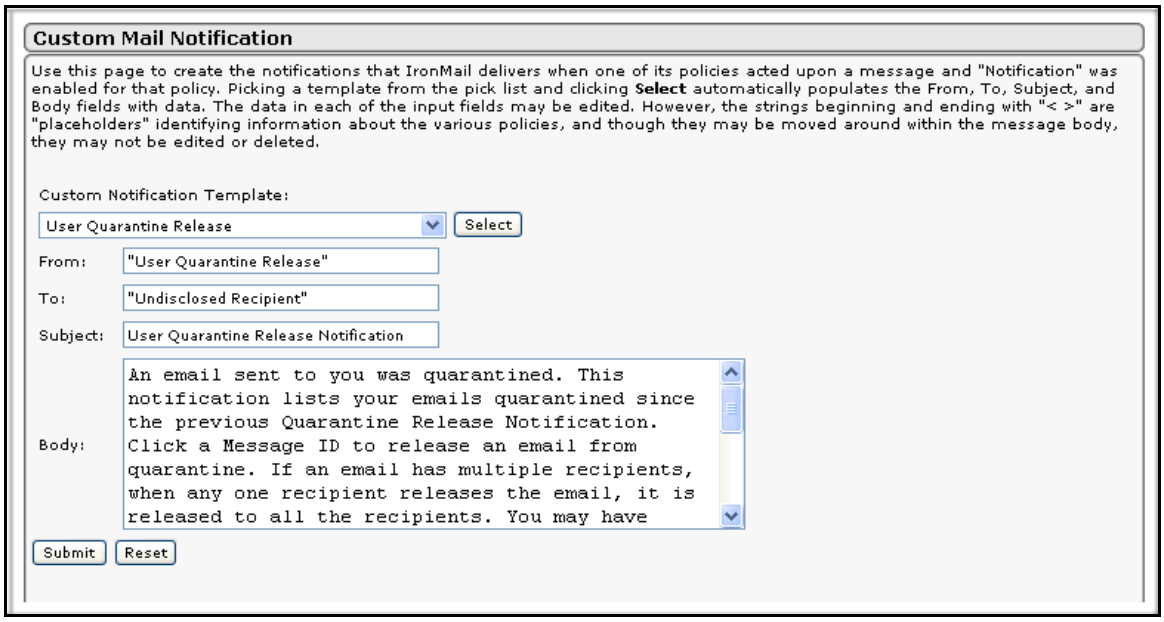
Field	Description
Apply To	Select the entity to which the rule will apply. • Email Address • Domain • User Group • Domain Group • Global
Data	To make a Message Stamping policy apply to a single individual, enter a valid email address in the User input field. (Multiple email addresses are not allowed in the **User** field. To apply a policy to more than one individual, create a group in *Policy Manager > Group Manager > Definition* and add individual users as required.) To create a policy applying a Message Stamping rule to a group of users, select the group name from the **Group** pick list. (All LDAP-imported groups as well as manually created groups are displayed in the pick list.) Note that a policy can only be applied to one group. To apply a policy to additional groups of users, separate policies must be created for each one. Note that the **Group** pick list contains the entry "Global." Select Global to apply the policy to everyone.
Exclude	Select the **Exclude** check box to apply the policy to everyone except the specified user or group. For example, if a rule states that outgoing messages from domain.com are to be stamped, and this policy is applied to david.scott@domain.com exclusively, then messages from everyone in domain.com except david.scott will be stamped.

Direction	An **Outbound Message Direction** radio button is selected by default and cannot be changed. By definition, IronMail only stamps outbound messages that it delivers for the internal mail servers it hosts.
Table of Rules	***The lower portion of the screen lists all existing rules that may be applied.***
ID	This column contains the unique ID for each rule. The ID is also a hyperlink that allows the rule to be edited.
Domain	This column lists the domain to which each rule is applied.
Footer Text	The footer text for the specific rule displays in this column.
Enable	Clicking the radio button associated with a rule enables that rule for the policy being created. Each policy may have only one rule enabled.

Mail Notification

Many of IronMail's policies provide an option to notify users if an IronMail *policy* performs an action on an email. The Custom Mail Notification page is where administrators may personalize the notification email that IronMail delivers to the user.

IronMail provides templates covering the policies that support user notification. Selecting a template for an IronMail policy populates text fields in the lower half of the page with sample text. The sample text may be edited and personalized as required.


Custom Mail Notification
Use this page to create the notifications that IronMail delivers when one of its policies acted upon a message and "Notification" was enabled for that policy. Picking a template from the pick list and clicking Select automatically populates the From, To, Subject, and Body fields with data. The data in each of the input fields may be edited. However, the strings beginning and ending with "< >" are "placeholders" identifying information about the various policies, and though they may be moved around within the message body, they may not be edited or deleted.
Custom Notification Template:
User Quarantine Release
Select
From:
"User Quarantine Release"
To:
"Undisclosed Recipient"
Subject:
User Quarantine Release Notification
Body:
An email sent to you was quarantined. This notification lists your emails quarantined since the previous Quarantine Release Notification. Click a Message ID to release an email from quarantine. If an email has multiple recipients, when any one recipient releases the email, it is released to all the recipients. You may have
Submit
Reset

Each template may contain one or more data elements—identified by open and closed angle brackets (<$textstring$>)—that reference elements of the policy, and the rules upon which they are based. IronMail will dynamically insert the appropriate data element from its database at the point in the message body where it appears. For example, a Mail Monitoring template may provide the following body:

> *This is an automatically generated Mail Monitoring notification. IronMail will automatically <$Action$> messages addressed to <$Data$>.*

If the Mail Monitoring policy stated that messages addressed to “competitor.com” are to be quarantined, the user receiving the email notification would see the following in his or email client:

> *This is an automatically generated Mail Monitoring notification. IronMail will automatically Quarantine messages addressed to competitor.com.*

The text within each of the data elements explain which part of the *rule* or policy it addresses. Administrators may copy and paste the data elements (in their entirety) anywhere within the notification’s body, but may not delete or edit them in any way. Doing so causes the email notification to fail.

After selecting a template, edit the text in the input fields.

From	Enter any text string in the From: input field. IronMail will insert this in the RFC822 From: header. Users will see in their email clients that the message originated from textstring (where “textstring” is the string entered in this field). An example of a text string for this From input field is "Postmaster.” For End User Quarantine notifications, when the system uses MS Exchange or Lotus Notes, the "from" entry will require some text inside quotation marks (e.g., "End User Administrator"). For End User Quarantine notifications when the system uses Groupwise, the "from" entry will require text within quotation marks and a valid address (e.g., "End User Administrator" <enduser@ct.com <mailto:enduser@ct.com>>).
To	Enter any text string in the To: input field. IronMail will insert this in the RFC822 To: header. Users will see in their email clients that the message is addressed to textstring (where “textstring” is the string entered in this field). Neither administrators nor IronMail can tell in advance who notifications will be sent to. Therefore, this To: value must be non-specific. An example of a text string for this To: input field is “Undisclosed Recipient.”
Subject	Enter any text string in the Subject: input field. IronMail will insert this in the RFC822 Subject: header. Users will see in their email clients that the Subject is textstring (where “textstring” is the string entered in this field. Administrators may wish to reference the IronMail policy responsible for generating the email notification. An example of a text string for this Subject: input field is “Mail Monitoring Policy Violation.”
Body	Each template populates the Body input field with a sample message, including any available data elements that notification supports. Edit the sample text or delete and create a new message, ensuring that the original data elements are not deleted or edited in any way. IronMail will place this in the body of the email notification it sends to the user, and insert the policy information that the data elements represent. An example of a text string for this Body: input field is “Our company does not allow messages to be delivered to “<$domain$>.” IronMail will performs a “<$action$>” action on these messages.”

Mail Monitoring and Encrypted Message Filtering Templates:

- <$Data$> will be the email address, domain, or group that required the action.
- <$Action$> will be a brief description of the policy’s action.

Off-Hour Delivery Template:

- <$Message Size$> will be the actual size of the message in bytes.
- <$Limit$> will be the Off-Hour Delivery limit in bytes. (This value will return nnnnnnn.0.)

- <$Delay in Hours$> will be the number of hours until the next "Begin Time" arrives.

Attachment Filtering Template:

- <$Data$> will be a file name or file extension.
- <$Action$> will be a brief description of the policy's action.

Content Filtering Template:

- <$Data$> will be the name of a dictionary.
- <$Action$> will be a brief description of the policy's action.

Secure Web Delivery Template:

- <$From$> will be the From address of the message sender.
- <$SLink$> will be the IronMail-generated HTTPS hyperlink the user will click to retrieve the message.

Anti-Virus Template:

- <$Virus Name$> will be the name of the detected virus.
- <$Virus Engine$> will be the name of the virus scanning engine (e.g., Sophos or McAfee).

SMTPO—Invalid Domain Template:

- <<$Domain$>> will the name of the domain the message was addressed to.

SMTPO—Invalid Domain, and Domain Name Same as Host Name Templates:

- <<$Domain$>> will the name of the domain the message was addressed to.

SMTPO—Domain Unreachable Template:

- <$Delivery Attempts$> will be the number of attempts IronMail has tried to deliver the message.

SMTPO - Domain Unreachable No More Attempts:

- IronMail will make no further attempts to deliver the message.

User Quarantine Release:

- IronMail will notify the user that the message(s) have been quarantined.

Note that IronMail generates a number of additional email notifications. The following messages are not configurable:

- **Forwarded:** When an IronMail policy has a "forward" action, it sends a message on to a forwarding email address and the original recipient does not receive the message. The message will be sent from "forwarded@default_domain.com."
- **Forwarded as Attachment:** When an IronMail policy has a "forward as attachment" action, it creates a new email envelope, with the original message as an attachment. The message will be sent from "fwd-attach@default_domain.com."
- **Copy:** When an IronMail policy has a "copy" action, it creates a new email envelope with the original message as an attachment. The message will be sent from "copied@default_domain.com."
- **Copied as Attachment:** When an IronMail policy has a "copy as attachment" action, IronMail creates a new email envelope with the original message as an attachment. The message will be sent from "copied-attach@default_domain.com."

- **Delivery Status Notification (DSN):** If IronMail is unable to deliver an email, and DSN is enabled in the SMTPO Service, it generates a new email to the sender. The DSN is sent from "dsn@default_domain.com."

  Note: Delivery Status Notifications may lose some fidelity with the Template if they are delivered to a Domino server. When the Domino SMTP listener receives a DSN, it recognizes it as DSN and reformats it to the Domino standard format. Then it places it in the server mail.box for delivery. The Notes form is also changed from "memo" to "NonDelivery Report."

- **Secure Web Delivery:** When Secure Web Delivery is enabled, IronMail generates a new email to the message recipient providing a hyperlink to the Secure Web Delivery host. The email is sent from "swm-postmaster@default_domain.com."
- **Reports:** If configured to do so, IronMail emails its daily Reports. They are sent from "reports@default_domain.com."
- **User-reported Spam to HQ:** If configured to do so, IronMail creates an email to CipherTrust's spam collection address, with user-reported spam as an attachment. The email is sent from "userreports@default_domain.com."
- **Enterprise Spam to HQ:** If configured to do so, IronMail creates an email to CipherTrust's spam collection address, with enterprise-reported spam as an attachment. The email is sent **from "enterprise@default_domain.com."**

Note: IronMail provides templates for customized email notifications when policies are enforced (for example, policies concerning Off-Hour Delivery, or enforcement of Mail Monitoring and Content Filtering rules, etc.). A notification message generated by IronMail is delivered by SMTPO to SMTPI services. The message generated by IronMail bypasses all the queues. At this point, the message has an RFC821 "From" address.

SMTP then sends the notifications to SMTPO for delivery to the intended recipient. When SMTPO delivers these outbound messages to the actual host for the recipient domain, the RFC821 "From" address is blank. All IronMail notifications are handled in this way. This approach prevents a possible looping email condition that can occur if generated notifications are sent with a "From Address" that is not reachable.

End User Quarantine

End User Quarantine Release

IronMail enables administrators to send notifications via email to internal end users when messages are quarantined because an IronMail *policy* condition was met. The notifications list the end user messages that are in the quarantine queue at a given point in time. By clicking the Message ID on a notification email, or by making selections from a message list window, users can release their messages for further processing. End User Quarantine Release can help to reduce the burden of releasing quarantined messages that may have been "false positives." It lets users manually and visually inspect the contents of IronMail's Quarantine Queues for the purpose of identifying and releasing email that was improperly identified as spam.

An administrator can create End User Quarantine Release policies based on a single user or a group of users and assign a list of quarantine queues that are included or excluded in the notification and release process.

Hyperlinks in the left navigation frame under Policy Manager allow navigation to the configuration options for IronMail's End User Quarantine Release.

EUQ Process Overview

Messages that have been quarantined must be validated so that notifications may be generated according to defined cycles. The process is split into two threads that may operate simultaneously.

The Identify Thread

The **identify** thread in the EUQ process runs every 15 minutes. It picks up all unprocessed messages from the quarantine queues, validates them, and inserts the required information into the **notified status** column in the **ct_eusr_qrelease** table. If the associated user already exists in the table and has a notification status of 0, the user ID is retrieved and the current message ID is inserted into the table with the user ID. If the user does not already exist, the thread writes a new record into the table (new user ID) with a notification status of 0, then adds the current message.

The identify thread also updates the **qrelease notified** column of the table for each message. The possible values for the updates are:

- 0 - the message is not yet processed
- 1 - the message has been validated, but does not qualify for notification
- 2 - the message qualifies for notification (these are the messages that will be picked up by the notify thread).

The Notify Thread

The **notify** thread wakes up on a user-defined schedule. This thread picks up all rows from the **ct_eusr_qrelease** table that have a notified status of 0. The process then generates notifications for these users for all qualified messages, and changes the **notified status** to 1.

Configure End User Quarantine

Administrators can configure notifications to end users when messages are quarantined and specify how often IronMail should check for quarantined messages.

By default, IronMail is configured to listen for SMTP connections addressed to the IP address specified in system configuration (*System > Configuration > IronMail > "IP Address"*). To use End User Quarantine (EUQ) Release, administrators must create a new "listening mechanism" so IronMail can also listen for connections from end users when they release quarantined messages. For this reason, this feature requires the creation of a "virtual" hostname and IP address for IronMail.

Administrators specify a virtual IP address and hostname using the Configure End User Quarantine screen so the EUQ Release can listen for the HTTPS request (on port 443). The virtual hostname is contained in the link sent to end users to return the request for release of quarantined messages. It allows IronMail to accommodate more than just SMTP connections and lets end users communicate with IronMail for EUQ Release. (For detailed information on how to create a virtual hostname and virtual IP address , refer to the Configure Server section in Secure Web Delivery.)

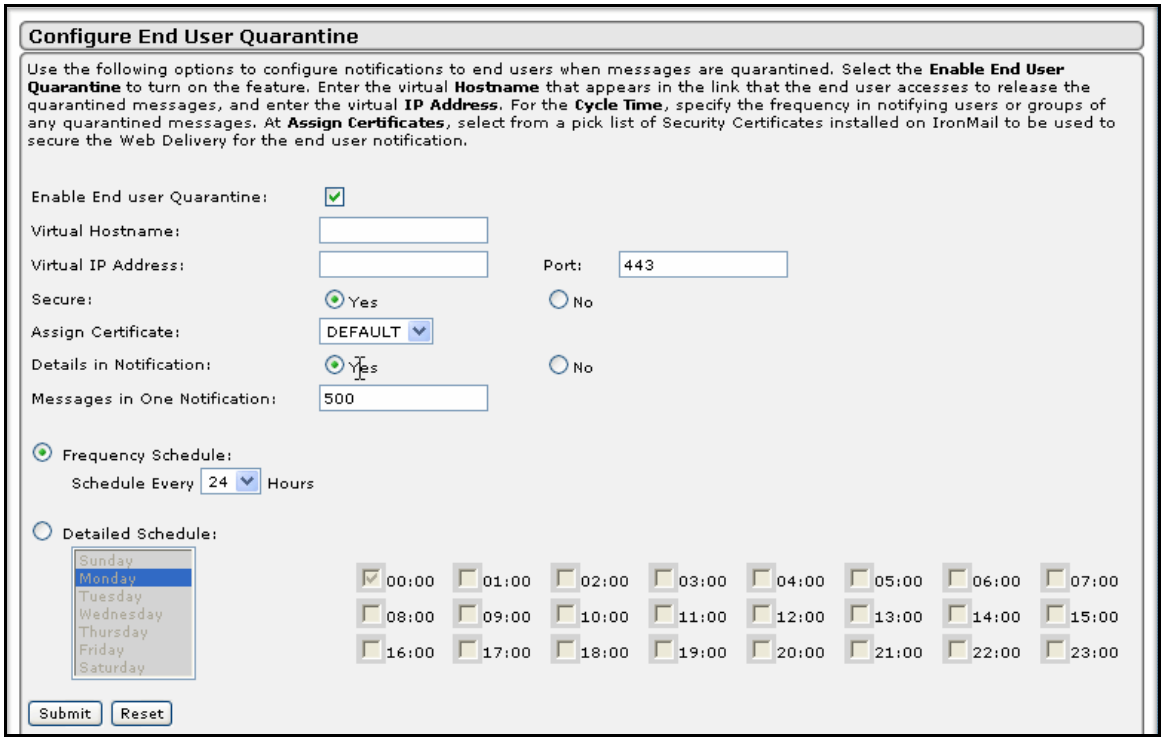
Be certain you do NOT use the underscore character ("_") in the virtual hostname you create. If you do use this character and the user clicks the "view all messages" link, the screen will display a blank list even if there are quarantined messages that should be listed.

For end users to access EUQ Release Notification messages through their browsers, they need to ensure that their workstations are pointing to a DNS server that can resolve the virtual *host name* used for EUQ, or they can place an entry in their local "hosts" file. This is applicable to environments where one DNS server is used by IronMail and a second used for End User workstations (internal and external DNS servers). If a workstation is unable to resolve the virtual hostname configured for EUQ, the End User will see the standard "The page cannot be displayed" error in their browser. Note that A and PTR records must be added for the virtual hostname configuration for EUQ Release. (For more information on implementing DNS, see the DNS Configuration section.)

Note: In a multiple IronMail environment, each IronMail configured for EUQ must use a unique virtual hostname and IP address to avoid ARP (Address Resolution *Protocol*) problems. Two IronMails must not use the same virtual hostname and virtual IP address.

As part of the EUQ configuration, administrators can select from a list of Security Certificates installed on IronMail to be used to secure the request sent from the browser to IronMail. To install the proper security certificate, administrators must install a certificate for the IronMail virtual host name used for EUQ Release Notification. This certificate should use the defined virtual host name to eliminate security alerts that occur when using the default IronMail host name . (For more information on how to install security certificates in IronMail, refer to information on the Certificate Manager.)

Note: A *firewall* reconfiguration may be required for EUQ to work correctly. Because quarantine release requests are returned to IronMail over port 443, administrators must open port 443 if users communicate with IronMail through a firewall. If users are not outside of a firewall, this port does not have to be opened.



Configuration options are::

Field	Description
Enable End User Quarantine	Select the **Enable End User Quarantine** check box to enable notification to end users when messages are quarantined.
Virtual Hostname	Enter a virtual hostname for the IronMail appliance. IronMail listens for this hostname when end users send a quarantine release request. This hostname appears in the link that the end user accesses to release the quarantined messages.
Virtual IP Address	Enter a virtual IP address for the IronMail appliance. IronMail listens for this IP Address when end users send a quarantine release request.

Port	Enter the port number through which release requests are to be returned to IronMail. Note: If all users are inside the firewall, this port identification is not required.
Secure	Select the appropriate radio button to indicate if messages are to be sent and received securely. Options are: • Yes • No
Assign Certificate	If End User Quarantine is enabled, select from a pick list of Security Certificates installed on IronMail to secure the request sent from the browser to IronMail. To install the proper security certificate, administrators must install a certificate for the IronMail virtual host name used for End User Release Notification. (For more information on how to install security certificates in IronMail, refer to information on the Certificate Manager.)
Details in Notification	Select the appropriate radio button to enable or suppress message details in notifications. Options are: • Yes - display of details is enabled. The notification emails the users receives will contain both the link to the table of all quarantined messages addressed to them • No - display of details is suppressed. The notification email will contain only the link to the quarantined message table.
Messages in One Notification	Enter a number between 1 and xxx to represent the maximum number of messages that may be included in a single notification.
Frequency Schedule	Clicking the radio button enables creation of a notification schedule. When the button is clicked, the user must also choose a frequency in hours from the drop-down list. Frequency may range from 1 to 72 hours between notification cycles. **Note:** The user must choose either Frequency Schedule or Detailed Schedule. Enabling one option disables the other.
Detailed Schedule	This option provides the means to create a detailed schedule for processing End User Quarantine notifications. This is done in two steps. • The left side of the screen displays a list of days. Select the day during which notices are to be sent. You may select only one day at a time. • On the right side, check boxes are provided for each of the 24 hours in a day. Clicking the check box for any hour of the day will enable IronMail to send EUQ notifications at that time. You may select from 0 to 24 notification times per day.

Click **Submit** to submit the entries or changes made on the Configure End User Quarantine screen. Click **Reset** to clear any input added since the last submission.

Policy Modifications for End User Quarantine Release

The point of EUQ Release Notification is to enable end users to users manually and visually inspect the contents of quarantined messages. For this reason, we recommend that administrators configure quarantine queues to disable the **automatic** processing of messages subject to end user quarantine release.

In the IronMail *Policy* Manager, you can enter a data value for the quarantine action to indicate how many days a message will be quarantined before IronMail delivers it. Any message with a quarantine value of zero is automatically deleted according to the Cleanup Schedule for Quarantine Data (*System > Cleanup Schedule*).

If users or groups do not release the messages on the Quarantine Release Notification, the messages are released or cleaned up (removed) according to the delivery schedule for the queue. Any messages in queues where messages are quarantined for a specified number of days are automatically submitted for processing in the next queue at the end of the quarantine period. To prevent the automatic processing and delivery of quarantined messages, administrators must set the quarantine value to zero.

Warning: Do not create an EUQR policy using a Domain-Based group. EUQR will compare the *domain name* in the domain-based group with the complete email address of the recipient address, and because they are different the recipients will not receive notifications. The only groups that should be used for creating policies are user-based groups (groups of individual email addresses) or the Global group. Note that EUQR is the only policy where IronMail compares the entire recipient address to the domain named in a group. Mail Monitoring, Encrypted Message Filtering, Content Filtering, Attachment Filtering, and Off-Hour Delivery policies may be applied to any recipient address whose domain matches the domain identified in a domain-based group.

Logging for the End User Quarantine Process

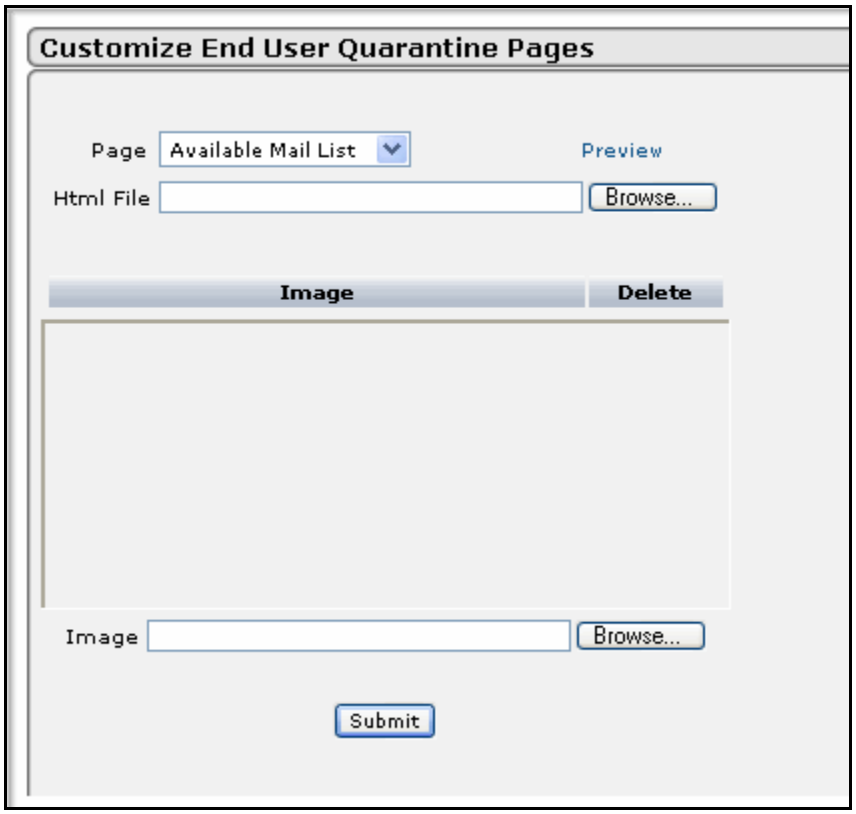
There are two logs pertaining to the EUQ Release process that are visible to administrators: eusrquarantine.log and ct_euser.log. These logs, which are viewable in the Command Line Interface, are useful for creating whitelist entries based on the messages releases by end users.

- **eusrquarantine:** The eusrquarantine.log shows the EUQ configuration and provides useful data on the message count, timestamp when the notifications were generated, and the total number of messages, for all users, that were quarantined since IronMail last generated a notification. Use the eusrquarantine.log to review the notified user count and sleep time if **Cycle Time** changes are needed in EUQ configuration.
- **ct_euser:** The ct_euser.log lists the messages released by end users. This is useful for creating whitelist entries based on the messages that users release. To search the log and display a list of messages that users released from the quarantine queues, use the following command:

  show log ct_euser | **grep** "Released Message"

Configure the EUQ Web Page

The End User Quarantine Notification page may be customized to promote the enterprise's company identity. More detailed information about customizing screens may be found in the Customizing Pages chapter of this manual.



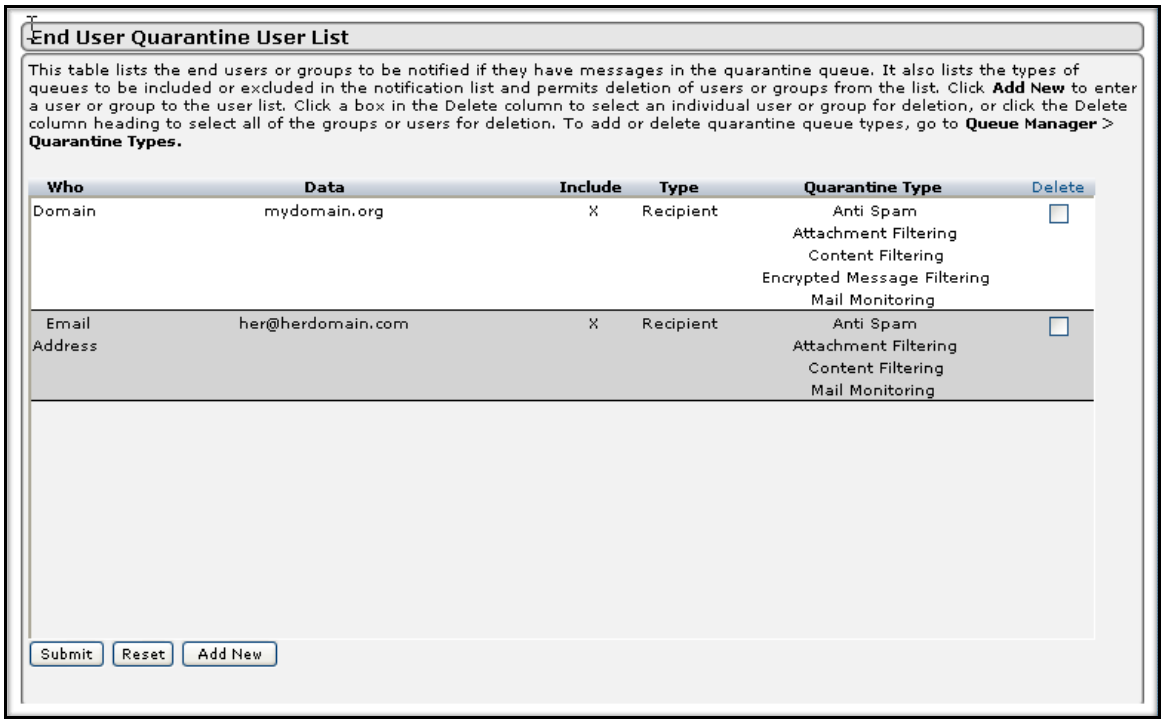
End User Quarantine User List

This table lists the active polices for end users or groups to be notified if they have messages in a configured quarantine queue. It displays the user type (Group or User), associated data (group name or individual email address), whether it is an include or exclude *policy*, and the Quarantine Types associated with the policy. The table also permits deletion of policies from the list.

In certain situations, a user on the End User Quarantine List can be a member of a *group* governed by one *rule* and, at the same time, have a slightly different rule applied to him/her. For example, a user may be a member of a group allowed to release messages from a Content Filtering queue, but there may also be a separate entry for that individual user permitting that user to release from ALL queues. In this case, user-based rules take precedence over group-based rules.

Note: The **Include** policy pertains to users and groups rather than queues.

Click **Add New** to add a new policy. Click a box in the **Delete** column to select individual policies for deletion, or click the **Delete** column heading to select all of the policies for deletion. (To add or delete quarantine queue types, go to *Queue Manager > Quarantine Types*.)


End User Quarantine User List
This table lists the end users or groups to be notified if they have messages in the quarantine queue. It also lists the types of queues to be included or excluded in the notification list and permits deletion of users or groups from the list. Click Add New to enter a user or group to the user list. Click a box in the Delete column to select an individual user or group for deletion, or click the Delete column heading to select all of the groups or users for deletion. To add or delete quarantine queue types, go to Queue Manager > Quarantine Types.
Who
Data
Include
Type
Quarantine Type
Delete
Domain
mydomain.org
X
Recipient
Anti Spam
Attachment Filtering
Content Filtering
Encrypted Message Filtering
Mail Monitoring
Email Address
her@herdomain.com
X
Recipient
Anti Spam
Attachment Filtering
Content Filtering
Mail Monitoring
Submit
Reset
Add New

The End User Quarantine User List displays the following information about the users or groups to be notified if they have messages in the quarantine queue.

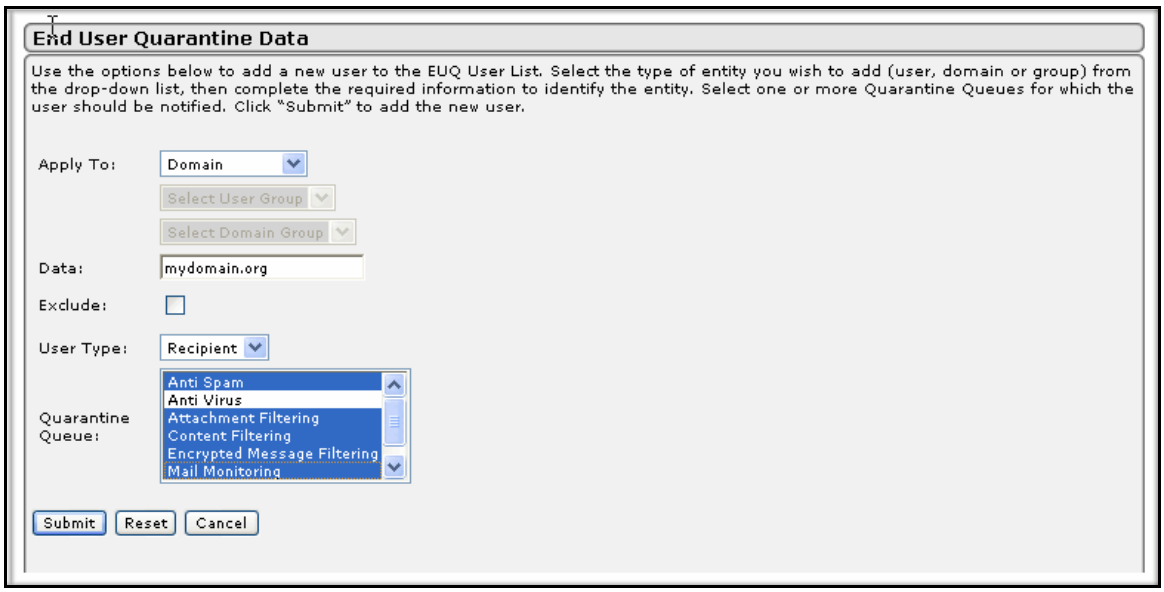
Who	Indicates if the End User is an individual User or Group. The **Who** entry qualifies the entry in the **Data** column.
Data	This column provides a value for the entry in the **Who** column. If "User" is in the **Who** column, **Data** identifies the email address of the user to be notified of a quarantined message. If "Group" is in the Who column, **Data** specifies the group whose users will be notified of quarantined messages.
Include	Identifies the users or groups to be included or excluded from receiving quarantined message notifications. Included groups or users are marked with an 'X' in the Include column. The Include/Exclude setting applies to users not queues. **Note:** If a policy excludes a user or group from receiving quarantine release notifications, by default all other users or groups that are not excluded are included. For example, if the Accounting group is excluded, everyone else is included.
Type	Select the Sender, Recipient, or Both to identify the user type.
Quarantine Type	The list of quarantine queues for which the user is to receive notification. **Warning:** Choosing the **Anti-Virus Quarantine Type** (or any quarantine queue that receives uncleaned messages) may result in the release of a virus by end users.
Delete	Click a Delete checkbox to mark a policy for deletion from the End User Quarantine List. Click the **Delete** column heading to select all of the policies for deletion.

Click **Submit** to delete the policies selected for deletion. Click **Reset** to clear the check boxes for users or groups selected for deletion.

Adding Users or Editing the User List

Click **Add New** to display the End User Quarantine Data window to add a new policy to the End User Quarantine List. The screen below allows the Administrator to update the user list.

Note: User entries may not be edited; they may only be added and deleted. To modify an existing entry, delete it and re-enter it with the changed information.


End User Quarantine Data
Use the options below to add a new user to the EUQ User List. Select the type of entity you wish to add (user, domain or group) from the drop-down list, then complete the required information to identify the entity. Select one or more Quarantine Queues for which the user should be notified. Click "Submit" to add the new user.
Apply To:
Domain
Select User Group
Select Domain Group
Data:
mydomain.org
Exclude:
User Type:
Recipient
Quarantine Queue:
Anti Spam
Anti Virus
Attachment Filtering
Content Filtering
Encrypted Message Filtering
Mail Monitoring
Submit
Reset
Cancel

Use the following fields to select users or groups to include or exclude in the quarantine queues monitored in the End User Quarantine list. For each user or group you can select one or more quarantine queues.

Apply To	Select to add a new user or group to the End User Quarantine List. If "User" is selected, add the user's email address in the Data field. If "Group" is selected, a pick list is enabled for selection of an existing group. This field will already be populated for an existing user entry.
Data	Enter the email address for the end user. This is only applicable if User is selected. Group names are automatically inserted in the Data field.
Exclude	Check the "Exclude" checkbox to the end users from receiving the quarantined message notification. **Note:** If a policy excludes a user or group from receiving quarantine release notifications, by default all other users or groups that are not excluded are included as recipients.
User Type	Select the Sender, Recipient, or Both to identify the user type.
Quarantine Queue	Select from the list of quarantine queues for which the end user is to receive notification. To select more than one queue, Shift-click or Control-click multiple items in this list. For information on how to configure additional types of quarantine queues, see Quarantine Types. **Warning:** Choosing the **Anti-Virus Quarantine Queue** (or any quarantine queue that receives uncleaned messages) may result in the release of a virus by end users.

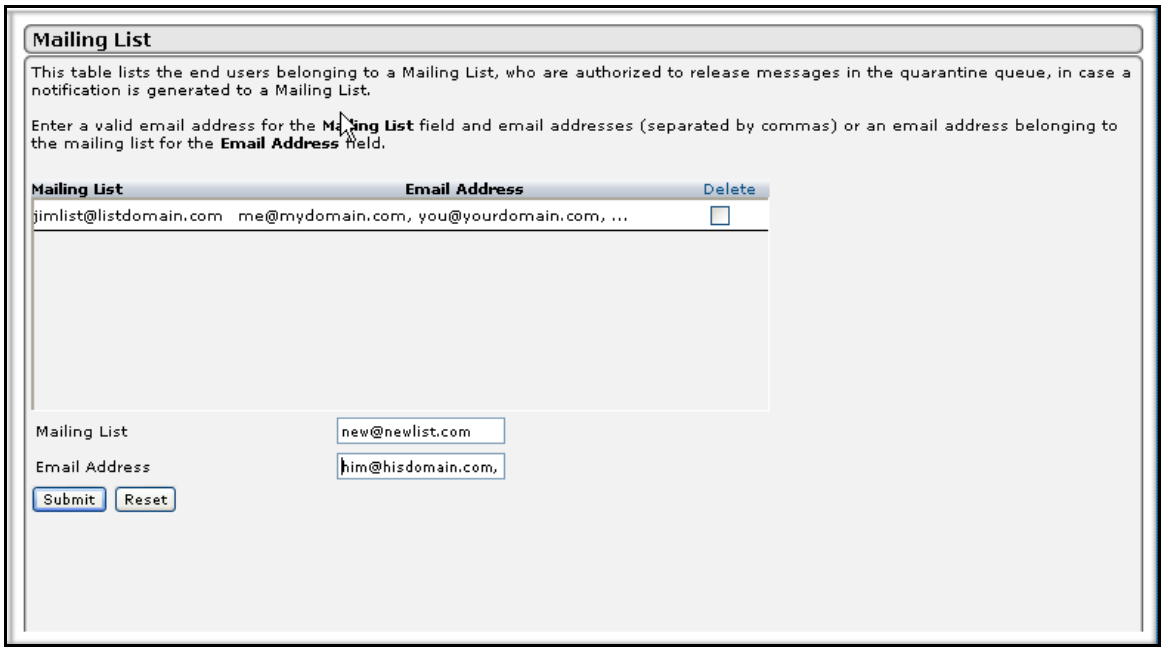
Click **Submit** to add the new policies to the End User Quarantine List. Click **Reset** to clear the entries and selections made on the End User Quarantine Data window. Click **Cancel** to close the window.

Warning: CipherTrust strongly warns against using an **Anti-Virus Quarantine Queue** (or any quarantine queue that receives uncleaned messages) in an End User Quarantine Release rule. If an Administrator includes an **Anti-Virus Quarantine Queue** in an End User Quarantine list, end users are able to release messages from the queue and process them with the message contents and any attachments unaltered. This can result in the end user releasing a virus.

EUQ Mailing List

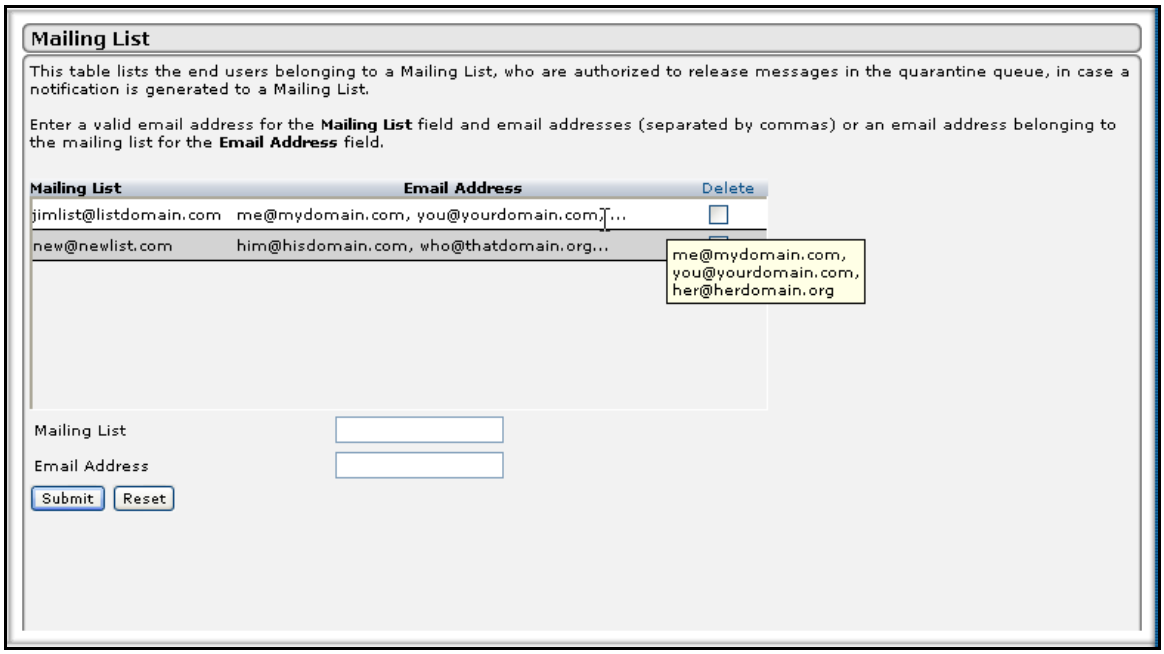
The Administrator may wish to set up mailing lists that will receive EUQ Notifications. A mailing list consists of one or more members, whose email addresses are listed as part of the mailing list. One notification email is sent to the mailing list, and is delivered to each member of that list. Any member of the list is authorized to release quarantined messages that appear in the notifications.

The screen below allows the Administrator to create and manage mailing lists.


Mailing List
This table lists the end users belonging to a Mailing List, who are authorized to release messages in the quarantine queue, in case a notification is generated to a Mailing List.
Enter a valid email address for the Mailing List field and email addresses (separated by commas) or an email address belonging to the mailing list for the Email Address field.
Mailing List
Email Address
Delete
jimlist@listdomain.com
me@mydomain.com, you@yourdomain.com, ...
Mailing List
new@newlist.com
Email Address
him@hisdomain.com,
Submit
Reset

Field	Description
Mailing List	This column lists all active mailing lists by main email address.
Email Address	The address column shows the beginning of the list of email addresses that are members of the mailing list. Rolling the cursor over this field displays a pop-up box detailing the email addresses.
Delete	Clicking the Delete check box and then clicking **Submit** will cause the associated mailing list to be deleted. Clicking the Delete hyperlink deletes all mailing lists.
Mailing List Field	To add and new mailing list, enter an email address for that list in the field.
Email Address Field	Enter one or more individual email addresses to include individuals as members of the mailing list.

Click **Submit** to activate any additions. If you have created a new list, the screen will display your new entry.


Mailing List
This table lists the end users belonging to a Mailing List, who are authorized to release messages in the quarantine queue, in case a notification is generated to a Mailing List.
Enter a valid email address for the Mailing List field and email addresses (separated by commas) or an email address belonging to the mailing list for the Email Address field.
Mailing List
Email Address
Delete
jimlist@listdomain.com
me@mydomain.com, you@yourdomain.com,...
new@newlist.com
him@hisdomain.com, who@thatdomain.org...
me@mydomain.com, you@yourdomain.com, her@herdomain.org
Mailing List
Email Address
Submit
Reset

Quarantine Release Notification

A Quarantine Release Notification is sent in the form of an email message generated for each user defined in an end user quarantine *policy* when they have messages in associated quarantine queues. The notification can contain the message headers for a maximum of 500 messages for a single end user. If a message is sent to a group of end users, it can be released by any one of them and the message is sent to all of the end users in the group. Similarly, if an email has more than one recipient (in the To, CC, or BCC fields), the quarantine release notification is delivered to ALL recipients. In addition, an end user will receive multiple notifications if they have multiple email aliases that have messages in quarantine. IronMail treats each alias as a separate address for the purposes of notification.

Warning: Do not create an EUQR policy using a Domain-Based group. EUQR will compare the *domain name* in the domain-based group with the complete email address of the recipient address, and because they are different the recipients will not receive notifications. The only groups that should be used for creating policies are user-based groups (groups of individual email addresses) or the Global group. Note that EUQR is the only policy where IronMail compares the entire recipient address to the domain named in a group. Mail Monitoring, Encrypted Message Filtering, Content Filtering, Attachment Filtering, and Off-Hour Delivery policies may be applied to any recipient address whose domain matches the domain identified in a domain-based group.

The quarantine queue is monitored according to the frequency set as the **Cycle Time** on the Configure End User Quarantine screen. Quarantine Release Notifications are sent to specified end users or groups after the quarantine queue is checked for any messages that have not yet triggered a notification. The end user or group is identified in the To: field of the notification email.

When the End User Quarantine query runs, it queries a maximum of 25,000 quarantined messages at a time, then sends notifications for that group of messages. Then the query runs again, querying the next 25,000 additional messages, and sends the notifications for that group. It continues in this manner until it has queried all messages that have been quarantined since the last time End User Quarantine Release (EUQR) was performed. This may result in two or more notifications to a single end user at the same time, if that user has messages in more than one group of 25,000 messages.

When the end user clicks on the ID entry in the Message ID column of the notification email, the message is released. Different pop-up messages appear depending on whether or not the message has been released prior to the user's current attempt.

- If the message was still in quarantine and is released by the current user, the pop-up window displays, "The message has been successfully released."
- If the message was sent to multiple recipients and one of them has already released the message, the pop-up window informs the current user, "The message you are trying to release has already been released. Please try another message."

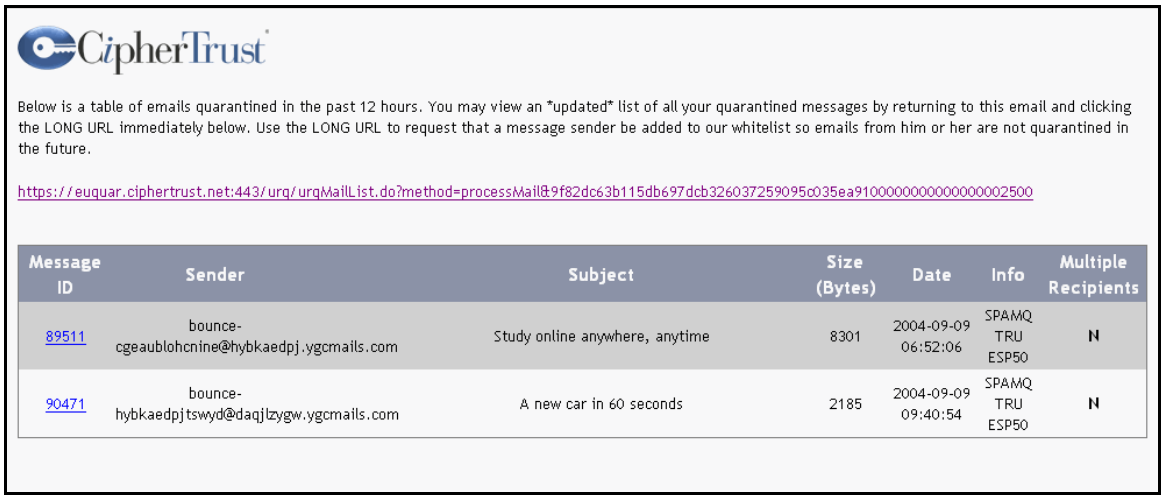
Note: Authentication is built into the URL that is sent out to the client. The URL is comprised of a unique random number for each notification, plus the user ID and the message ID. For authentication we check the length of the URL to see if it was tampered with, and match the combination of three parameters (the random number, user ID and message ID) with what exists in the datastore for the user. If any one of the parameters fails to match, IronMail generates an Invalid User exception.

If the message is released by the user, or if the message was already released to another user in a recipient group, a pop-up window is displayed indicating that the message was successfully delivered. If the message has already been removed in a scheduled IronMail cleanup cycle, a pop-up window displays an error notice.

Note: If the end-user has installed a pop-up blocker, it may prevent the display of pop-up windows used in End User Quarantine Release. To avoid blocking IronMail pop-ups, disable or override the pop-up blocker.

An end user can also use the link at the top of the release notification to view a list of all of his or her quarantined messages then select one or more messages from the quarantine queue and release them for delivery. Accessing this link shows all messages in the monitored Quarantine Queues for the user, not just the one in the associated email.

Note: Administrators can include all Quarantine Queues in their policies. End users can see a list of their messages that are in the Quarantine Queues except for messages in the Outbound Quarantine Queue, Off Hour Queue, and Failure Queue.



CipherTrust

Below is a table of emails quarantined in the past 12 hours. You may view an *updated* list of all your quarantined messages by returning to this email and clicking the LONG URL immediately below. Use the LONG URL to request that a message sender be added to our whitelist so emails from him or her are not quarantined in the future.

https://euquar.ciphertrust.net:443/urq/urqMailList.do?method=processMail&9f82dc63b115db697dcb326037259095c035ea91000000000000000002500

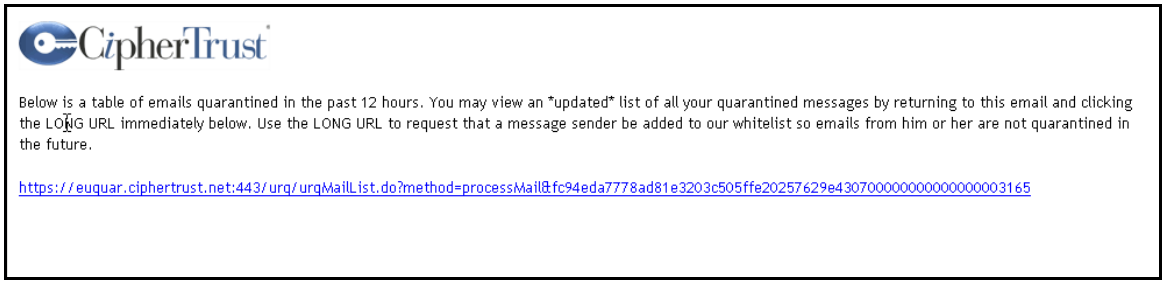
Message ID	Sender	Subject	Size (Bytes)	Date	Info	Multiple Recipients
89511	bounce-cgeaublohcnine@hybkaedpj.ygcmails.com	Study online anywhere, anytime	8301	2004-09-09 06:52:06	SPAMQ TRU ESP50	N
90471	bounce-hybkaedpjtswyd@daqjlzygw.ygcmails.com	A new car in 60 seconds	2185	2004-09-09 09:40:54	SPAMQ TRU ESP50	N

The automatically generated Quarantine Release Notification (if Details in Notification is enabled in the Configure End User Quarantine window) shows the following information for each message that is quarantined for end users.

Message ID	This column displays a number that uniquely identifies the message. Clicking on the ID in this column releases the message. IronMail then displays a

	confirmation window to the end user.
Sender	This column displays the RFC821 From address of the message sender.
Subject	This column displays the message's Subject Line.
Size in Bytes	This column displays the message's size.
Date	This column displays the timestamp when IronMail received the message.
Info	This column identifies the name of the quarantine queue where the message for the end user is quarantined. Messages in the outbound quarantine queue are not included in the End User Quarantine Release feature and are not listed in this notification.

If Details in Notification is disabled, the EUQ Notice only contains the link and the introductory message.

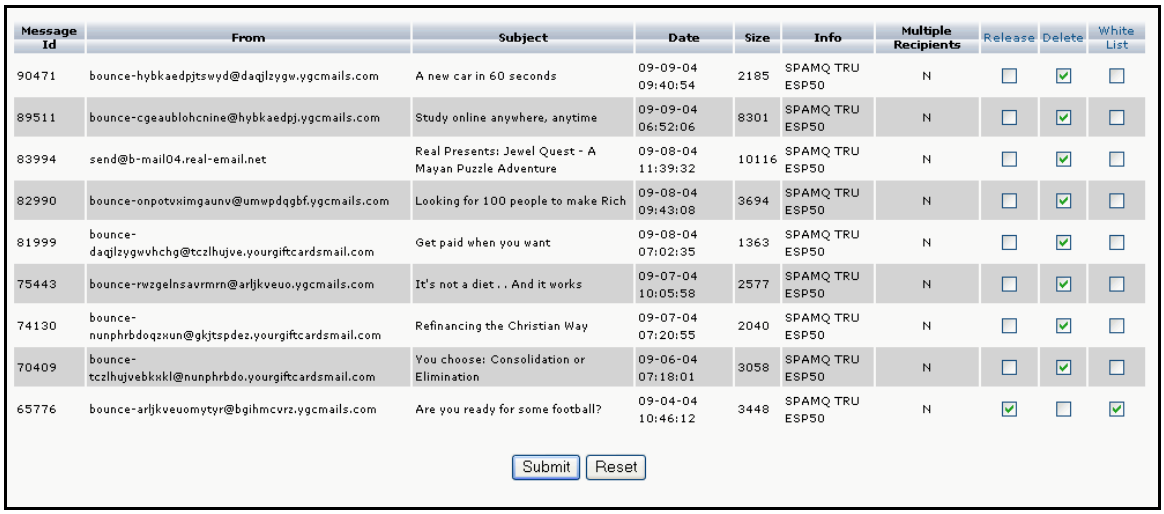

CipherTrust
Below is a table of emails quarantined in the past 12 hours. You may view an *updated* list of all your quarantined messages by returning to this email and clicking the LONG URL immediately below. Use the LONG URL to request that a message sender be added to our whitelist so emails from him or her are not quarantined in the future.
https://euquar.ciphertrust.net:443/urq/urqMailList.do?method=processMail&fc94eda7778ad81e3203c505ffe20257629e430700000000000000003165

To release a listed message from a quarantine queue, click the message ID in the Message ID column. The user's browser establishes a secure connection with the IronMail server.

Both the notification itself and the screen that appears when the user wants to view a list of all quarantined messages contain in indicator that lets the user know if the message has multiple recipients. This information may influence the decision to release the message, since all recipients will receive it once it is released.

Viewing a List of All Quarantined Messages

To view a list of all quarantined messages for an end user, click the hyperlink at the top of the notification email. All quarantined messages that have been validated and found to qualify for notification and for which notice has not been sent will show on the user's screen. Messages that are released or processed do not appear on the list of all quarantined messages for the user.



Message Id	From	Subject	Date	Size	Info	Multiple Recipients	Release	Delete	White List
90471	bounce-hybkaedpjtswyd@daqjlzygw.ygcmails.com	A new car in 60 seconds	09-09-04 09:40:54	2185	SPAMQ TRU ESP50	N	☐	☑	☐
89511	bounce-cgeaublohcnine@hybkaedpj.ygcmails.com	Study online anywhere, anytime	09-09-04 06:52:06	8301	SPAMQ TRU ESP50	N	☐	☑	☐
83994	send@b-mail04.real-email.net	Real Presents: Jewel Quest - A Mayan Puzzle Adventure	09-08-04 11:39:32	10116	SPAMQ TRU ESP50	N	☐	☑	☐
82990	bounce-onpotvximgaunv@umwpdqgbf.ygcmails.com	Looking for 100 people to make Rich	09-08-04 09:43:08	3694	SPAMQ TRU ESP50	N	☐	☑	☐
81999	bounce-daqjlzygwvhchg@tczlhujve.yourgiftcardsmail.com	Get paid when you want	09-08-04 07:02:35	1363	SPAMQ TRU ESP50	N	☐	☑	☐
75443	bounce-rwzgelnsavrmrn@arljkveuo.ygcmails.com	It's not a diet . . And it works	09-07-04 10:05:58	2577	SPAMQ TRU ESP50	N	☐	☑	☐
74130	bounce-nunphrbdoqzxun@gkjtspdez.yourgiftcardsmail.com	Refinancing the Christian Way	09-07-04 07:20:55	2040	SPAMQ TRU ESP50	N	☐	☑	☐
70409	bounce-tczlhujvebkxkl@nunphrbdo.yourgiftcardsmail.com	You choose: Consolidation or Elimination	09-06-04 07:18:01	3058	SPAMQ TRU ESP50	N	☐	☑	☐
65776	bounce-arljkveuomytyr@bgihmcvrz.ygcmails.com	Are you ready for some football?	09-04-04 10:46:12	3448	SPAMQ TRU ESP50	N	☑	☐	☑

Submit Reset

The list of all messages in quarantine for a particular user shows the following information for each message.

Field	Description
Message ID	The system assigns a unique ID number to every message coming into IronMail. This column displays these numbers for quarantined messages.
From	This column displays the RFC821 From address of the message sender.
Subject	This column displays the message's Subject Line.
Date	This column displays the timestamp when IronMail received the message.
Size	This column shows the size of each quarantined message in bytes.
Info	This column lists the queue where each message is being quarantined.
Multiple Recipients	If the message is addressed to more than one individual, this column will display a "Yes" for that message. If not, "No" will display.
Release	Click a box in the Release column to select individual messages to release. Messages are not released until the user clicks the **Submit** button at the bottom of the screen. Clicking the Release hyperlink will cause all messages in the list to be released.
Delete	Click a box in the Delete column to select individual messages to be deleted. Messages are not deleted until the user clicks the **Submit** button at the bottom of the screen. Clicking the Delete hyperlink will cause all messages in the list to be released.
Whitelist	Click a box in the Whitelist column to request that the sender or sending domain of the inbound individual messages be whitelisted for this user, as well as messages going out from himself/herself to specific individuals or domains. Requests are not sent until the user clicks the **Submit** button at the bottom of the screen. Clicking the Whitelist hyperlink will cause whitelisting to be requested for all senders in the list. **Note:** EUQ Whitelisting may be configured in such a way that end user requests automatically result in whitelisting, or so that the requests must be processed by the Administrator. In either case, the Administrator has oversight of the whitelisting process.

The user can delete messages using this screen by submitting a delete request. If the message has only one recipient (the user who submitted the request), the message is dropped. If the message has multiple recipients, the current user is removed from the list.

Note: The hyperlink that displays the list of all quarantined messages may not work with MS Outlook OWA 2003. This problem exists when signature protection is enabled, with the specific signature #1054 (WEB-MISC weblogic view source attempt) enabled as well. If the problem occurs, the Administrator can resolve it by disabling the signature.

Customizing Release Notifications

IronMail provides a template for the message text that IronMail delivers to users receiving quarantine release notifications. Administrators may customize the notifications by editing the text shown on the lower half of the Custom Mail Notification page.

The notification may be broken down into three parts: the text, the main link, and the records. The template mentioned above allows the user to customize the contents of the text part. Additionally, the Administrator can set the order of appearance of the three parts.

Security Certificate Error Messages During End User Quarantine Release Notification

When users release a quarantined message, a Security Alert may appear telling them that their security certificate is incorrect. This occurs if the correct security certificate is not installed for End User Quarantine Release Notification using the Configure End User Quarantine window. Users can continue to release their quarantined messages without the certificate, but the Security Alerts may result in unnecessary user support inquiries.

To install the proper security certificate, administrators must install a certificate for the IronMail virtual *host name* used for End User Quarantine Release. This is different from the usual certificate installed for the IronMail host name. (For more information on how to install security certificates in IronMail, refer to information on the Certificate Manager.)

Consolidating Notifications

In environments where multiple IronMail appliances are deployed, an end user may receive multiple notifications due to quarantined messages on more than one appliance. This possibility can be alleviated by consolidating the notifications. This requires that one separate appliance be configured as the EUQ box. This is an appliance with the End User Quarantine feature enabled, and with queues configured identically to the other IronMails.

The other IronMails in the system will reroute their messages to the EUQ box if they want the messages quarantined and notifications generated for them. These other IronMails will not have EUQ enabled. A configuration option on each IronMail will denote if the messages are to be quarantined on the original appliance or rerouted to the EUQ appliance.

When messages are rerouted, an new RFC822 header will be added to indicate the queues that have processed each message, the queue to which is should go, and perhaps additional information. The RIP Queue on the EUQ appliance then processes the headers and writes the messages to the appropriate queues. After processing, the added headers are removed. The messages will be processed the same way as those on individual IronMail appliances. The notification process applies as defined earlier, and released messages will proceed through the remaining queues as normal.

Note: This feature is restricted to messages quarantined by MMQ, CFQ and SpamQ.

End User Whitelists

EUQ Whitelisting

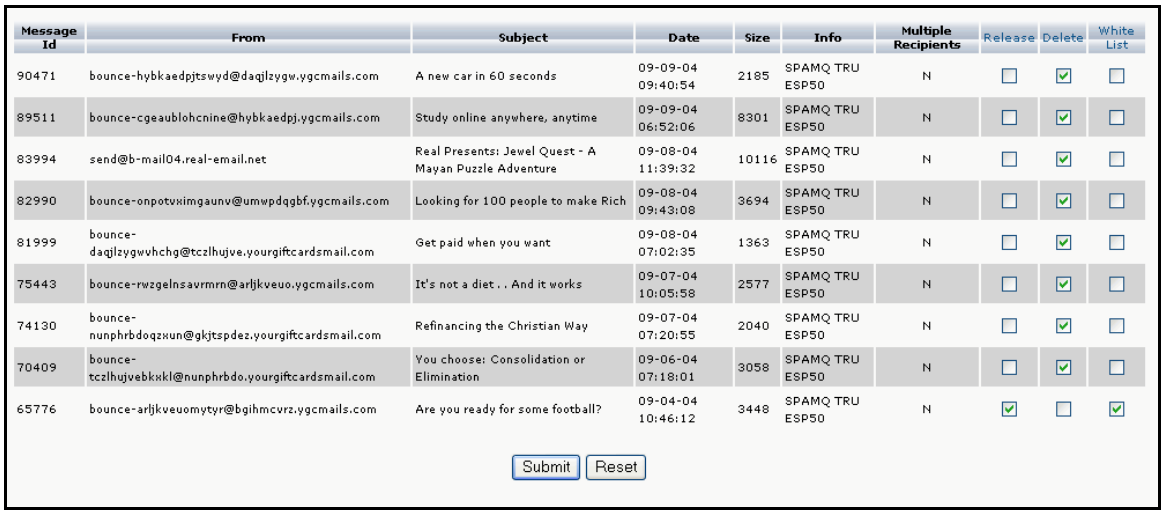
End User Quarantine Whitelisting allows users to whitelist rules and policies that apply only to themselves. They base these rules and policies on the quarantined messages for which they receive EUQ notifications. This ability can relieve some of the Administrative burden associated with maintaining whitelists while still allowing the means for administrative oversight when appropriate.

When a user receives notification of a quarantined message for which a whitelist entry is desirable, the user submits a request to whitelist either the email address or the domain associated with that message. Either the sender or the recipient (when the end user is the sender) of the message may be whitelisted. In other words, the user may whitelist messages coming in from specific senders or domains or messages going out to specific users or domains. In either case, the messages will be allowed to bypass specific IronMail processes.

IronMail can be configured to accept whitelist entries automatically or manually.

Automatic Processing

If EUQ Whitelisting is enabled and is configured for automatic whitelisting, the end user can create whitelist entries without the Administrator's assistance. When the user receives a notification and then clicks the main link on the notification email, a complete list of all quarantined messages for that user displays. This screen includes the provision for requesting a whitelist entry for each message shown.



Message Id	From	Subject	Date	Size	Info	Multiple Recipients	Release	Delete	White List
90471	bounce-hybkaedpjtswyd@daqjlzygw.ygcmails.com	A new car in 60 seconds	09-09-04 09:40:54	2185	SPAMQ TRU ESP50	N	☐	☑	☐
89511	bounce-cgeaublohcnine@hybkaedpj.ygcmails.com	Study online anywhere, anytime	09-09-04 06:52:06	8301	SPAMQ TRU ESP50	N	☐	☑	☐
83994	send@b-mail04.real-email.net	Real Presents: Jewel Quest - A Mayan Puzzle Adventure	09-08-04 11:39:32	10116	SPAMQ TRU ESP50	N	☐	☑	☐
82990	bounce-onpotvximgaunv@umwpdqgbf.ygcmails.com	Looking for 100 people to make Rich	09-08-04 09:43:08	3694	SPAMQ TRU ESP50	N	☐	☑	☐
81999	bounce-daqjlzygwvhchg@tczlhujve.yourgiftcardsmail.com	Get paid when you want	09-08-04 07:02:35	1363	SPAMQ TRU ESP50	N	☐	☑	☐
75443	bounce-rwzgelnsavrmrn@arljkveuo.ygcmails.com	It's not a diet . . And it works	09-07-04 10:05:58	2577	SPAMQ TRU ESP50	N	☐	☑	☐
74130	bounce-nunphrbdoqzxun@gkjtspdez.yourgiftcardsmail.com	Refinancing the Christian Way	09-07-04 07:20:55	2040	SPAMQ TRU ESP50	N	☐	☑	☐
70409	bounce-tczlhujvebkxkl@nunphrbdo.yourgiftcardsmail.com	You choose: Consolidation or Elimination	09-06-04 07:18:01	3058	SPAMQ TRU ESP50	N	☐	☑	☐
65776	bounce-arljkveuomytyr@bgihmcvrz.ygcmails.com	Are you ready for some football?	09-04-04 10:46:12	3448	SPAMQ TRU ESP50	N	☑	☐	☑

Submit Reset

Field	Description
Message ID	The system assigns a unique ID number to every message coming into IronMail. This column displays these numbers for quarantined messages.
From	This column displays the RFC821 From address of the message sender.
Subject	This column displays the message's Subject Line.
Date	This column displays the timestamp when IronMail received the message.
Size	This column shows the size of each quarantined message in bytes.
Info	This column lists the queue where each message is being quarantined.

Multiple Recipients	If the message is addressed to more than one individual, this column will display a "Yes" for that message. If not, "No" will display.
Release	Click a box in the Release column to select individual messages to release. Messages are not released until the user clicks the **Submit** button at the bottom of the screen. Clicking the Release hyperlink will cause all messages in the list to be released.
Delete	Click a box in the Delete column to select individual messages to be deleted. Messages are not deleted until the user clicks the **Submit** button at the bottom of the screen. Clicking the Delete hyperlink will cause all messages in the list to be released.
Whitelist	Click a box in the Whitelist column to request that the sender or sending domain of the inbound individual messages be whitelisted for this user, as well as messages going out from himself/herself to specific individuals or domains. Requests are not sent until the user clicks the **Submit** button at the bottom of the screen. Clicking the Whitelist hyperlink will cause whitelisting to be requested for all senders in the list. **Note:** EUQ Whitelisting may be configured in such a way that end user requests automatically result in whitelisting, or so that the requests must be processed by the Administrator. In either case, the Administrator has oversight of the whitelisting process.

The user may choose one or more messages to be whitelisted. A *rule* is then created for the sender or the recipient (email address or domain), and is applied to the user who is doing the whitelisting.

In the case that two or more users create a whitelist entry for the same value (same sender or recipient), IronMail creates only one rule for that entry, and then applies it to all the users who have requested it.

Note: User-created whitelist entries will not be visible in the User Interface because the lists are expected to grow beyond a size that can be displayed. A search facility will be available to the Administrator, allowing review of a subset of the list. The Administrator can select entries that need to be deleted.

Manual Processing

If EUQ is enabled and is configured for manual whitelisting, the end users will still submit requests in the same way as for automatic processing. However, instead of automatically creating whitelist entries, the requests are submitted to the database and are available to the Administrator on the UI (*Policy Manager > White Listing > new screen*). The Administrator will have the ability to submit both the rule and the policy. He or she may apply the rule to the user who created the request, in which case the rule will be considered user-created; or the user may be allowed to specify to whom the rule should apply, but allow the Administrator to actually apply it. This is helpful when the Administrator needs to apply the same rule for more than one user. This latter option is considered an administrator-created rule.

Maintaining EUQ Whitelists

Keeping the Whitelists up to date and functioning properly requires maintenance activity. If more than one IronMail appliance is deployed, the whitelists must be synchronized to assure they are applied correctly. Whitelist usage updates must be propagated as well, as do deletions requested by the users or the Administrator. And, finally, regular automated cleanup is necessary to ensure that only those rules and policies that are truly useful remain in the whitelists.

Synchronization

In an environment with more than one IronMail appliance, the whitelists must be synchronized. Rules created in one IronMail by a user need to be propagated to all others in the system. Each IronMail must recognize all others from which it may receive entries.

Synchronization action only synchronizes end-user whitelists. Synchronization of Administrator-generated whitelist entries are synchronized by using the Back and Restore functionalities in the System program area.

When a user issues a whitelist request from a notification, the pertinent data is stored in a temporary table on the IronMail where it was generated. At a pre-determined time, all the whitelist entries are collected and then propagated in batches of 100 to the other IronMails in the system. SMTPProxy on the recipient IronMail receives the request to add the new entry, stores it temporarily, and then moves it to the primary whitelist location at periodic intervals. At these intervals it also reconfigures the RIP Queue to recognize the newly added entries.

A retry mechanism is available if propagation fails for any reason.

Note: To ensure uniformity of all whitelists in the system, CipherTrust strongly recommends that all existing whitelists be synchronized before enabling this feature. All subsequent synchronization is performed on new user entries added or deleted. The import and export options in whitelisting can be used to accomplish this requirement.

Scheduled Cleanup

A second requirement for maintaining accurate whitelists is the elimination of unused rules. The `ct_bypass` table includes a time column that is updated to show the last access time each time a message qualifies for a user-created whitelist *rule*. An automatic cleanup process reviews the table and deletes any entries that have not been used for a user-defined period of time. The user-created policies that apply these rules are altered accordingly. If the rule is the only rule in a *policy*, the policy is deleted as well. If this is not the case, the rule is deleted and the rule ID is removed from the policy.

RIP Queue causes a list of bypass rules that have been triggered when it processes a message. This list is the source for access times. The database information is updated a pre-configured number of minutes (every 60 minutes).

The automatic cleanup process is enabled or disabled by the Administrator.

Usage Updates

In multiple-IronMail environments, where messages can flow through any appliance, the usage information for each rule must be propagated to all IronMails in the system. This keeps the usage information for all rules in synch on all the appliances. This update is performed in batches at the end of the day.

Deletions

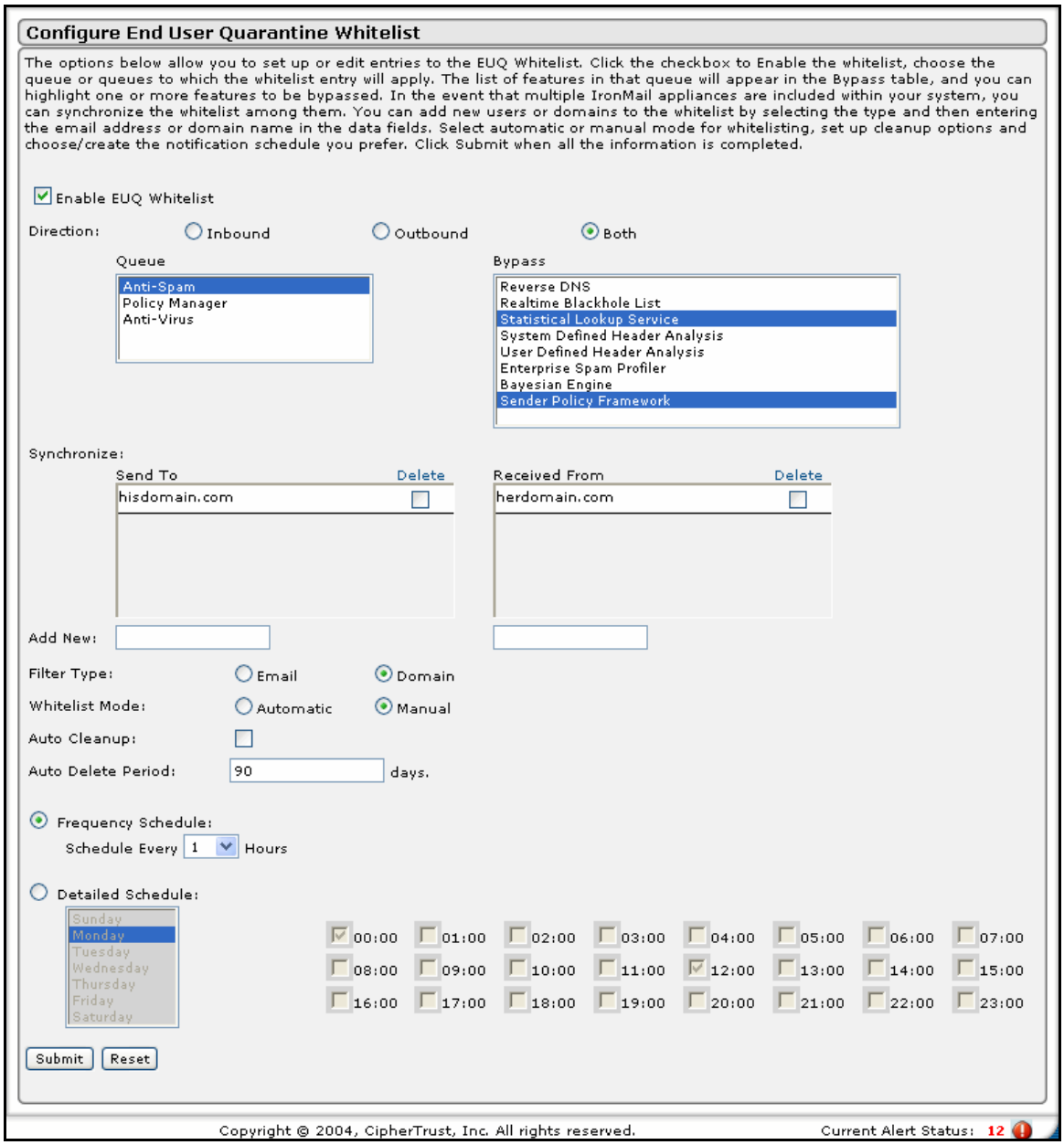
End users may request that any rules they have created be deleted, but the deletions have to be performed by the Administrator. The Administrator has the capability to search for the rule and to eliminate it; the search may be performed against rule information or policy information, against user-created rules and policies, or against administrator-created rules and policies. The Administrator can choose the rules and users that should be deleted. The deletions will be accomplished the next time the cleanup process runs. The Administrator also has the option to force the deletions to occur immediately and to force immediate synchronization. If the rule is the only rule in a policy, the policy is deleted as well. If this is not the case, the rule is deleted and the rule ID is removed from the policy.

The Administrator may also delete rules that have been requested but have not yet been applied, under either the automatic or the manual processing mode, when viewing them in the GUI. The user can also view the requests and mark for deletion any that need not be submitted. The UI will then remove the requests.

Configure EUQ Whitelists

Whitelisting from the GUI

End User Quarantine Whitelisting is requested by the end user based upon the EUQ notifications received.

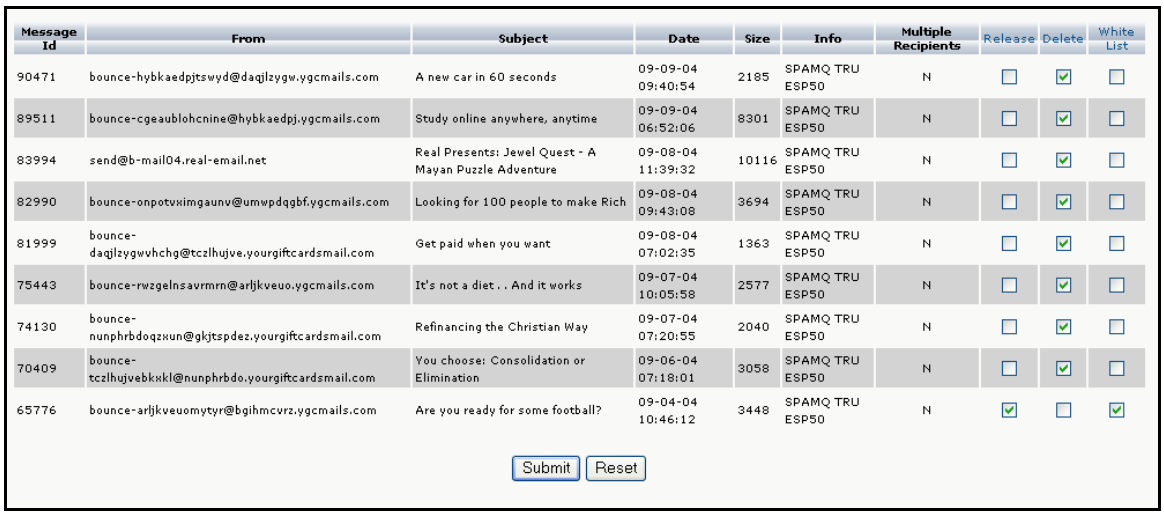


Field	Description
Enable EUQ Whitelist	Clicking the checkbox enables the EUQ whitelist feature, allowing end users to request whitelist entries.
Direction	Click the appropriate radio button to indicate the message direction for entries included in the whitelist: inbound, outbound, or both.

Queue and Bypass	Select the queue to which the whitelist rule is to apply, then select the feature or features within that queue that messages will be allowed to bypass. Repeat the process for additional queues as necessary.
Synchronize	The two tables (Send To and Receive From) contain domain names for the domains that need to maintain the same end-user whitelists. Synchronization assures that the whitelists recognized by each domain (each separate IronMail appliance) are identical. The Send To domains are those to which this IronMail must send synchronization information. The Receive From domains are those from which it must receive information. Only end-user generated whitelists are synchronized.
Add New	Add new domains to either table by entering the domain names and clicking **Submit**.
Filter Type	Select the filter type for this whitelist. Are the entries to be whitelisted based upon email addresses or domains?
Whitelist Mode	Select the mode for creation of whitelist entries for this list. Options are: • Automatic - IronMail will automatically create a whitelist entry for each request it receives. This is NOT the recommended mode of operation. • Manual - The Administrator must create the entries from each request. This allows the Administrator to monitor the entries and to determine if custom application is in order (e.g., if more than one user has requested the same whitelist entry). This is the recommended mode.
Auto Cleanup	Selecting the Auto Cleanup checkbox enables IronMail to eliminate rules that have not been applied for the configured delete period.
Auto Delete Period	Enter a time in days that rules should remain in effect without being deleted even if they have not been applied. Unused rules older than this number of days will be deleted by the Auto Cleanup function.
Frequency Schedule **or** **Detailed Schedule**	Determine the frequency for Auto Cleanup to run. You may select a frequency schedule based on an elapsed time in hours by clicking the Frequency Schedule click box and then selecting the time between runs. You may also choose to specify the times for Auto Cleanup on a specific schedule by choosing a day and selecting the cycle times for that day, and repeating the selection process for other days until you have completed the desired schedule.

Requesting User-Generated Whitelist Entries

When the user clicks on the main link as indicated on the notification email, a list of all that user's quarantined messages displays. If the EUQ Whitelisting function is enabled, the screen will include check boxes for each message. Checking one or more of these boxes can result in requests for whitelist entries.



Message Id	From	Subject	Date	Size	Info	Multiple Recipients	Release	Delete	White List
90471	bounce-hybkaedpjtswyd@daqjlzygw.ygcmails.com	A new car in 60 seconds	09-09-04 09:40:54	2185	SPAMQ TRU ESP50	N	☐	☑	☐
89511	bounce-cgeaublohcnine@hybkaedpj.ygcmails.com	Study online anywhere, anytime	09-09-04 06:52:06	8301	SPAMQ TRU ESP50	N	☐	☑	☐
83994	send@b-mail04.real-email.net	Real Presents: Jewel Quest - A Mayan Puzzle Adventure	09-08-04 11:39:32	10116	SPAMQ TRU ESP50	N	☐	☑	☐
82990	bounce-onpotvximgaunv@umwpdqgbf.ygcmails.com	Looking for 100 people to make Rich	09-08-04 09:43:08	3694	SPAMQ TRU ESP50	N	☐	☑	☐
81999	bounce-daqjlzygwvhchg@tczlhujve.yourgiftcardsmail.com	Get paid when you want	09-08-04 07:02:35	1363	SPAMQ TRU ESP50	N	☐	☑	☐
75443	bounce-rwzgelnsavrmrn@arljkveuo.ygcmails.com	It's not a diet . . And it works	09-07-04 10:05:58	2577	SPAMQ TRU ESP50	N	☐	☑	☐
74130	bounce-nunphrbdoqzxun@gkjtspdez.yourgiftcardsmail.com	Refinancing the Christian Way	09-07-04 07:20:55	2040	SPAMQ TRU ESP50	N	☐	☑	☐
70409	bounce-tczlhujvebkxkl@nunphrbdo.yourgiftcardsmail.com	You choose: Consolidation or Elimination	09-06-04 07:18:01	3058	SPAMQ TRU ESP50	N	☐	☑	☐
65776	bounce-arljkveuomytyr@bgihmcvrz.ygcmails.com	Are you ready for some football?	09-04-04 10:46:12	3448	SPAMQ TRU ESP50	N	☑	☐	☑

Submit Reset

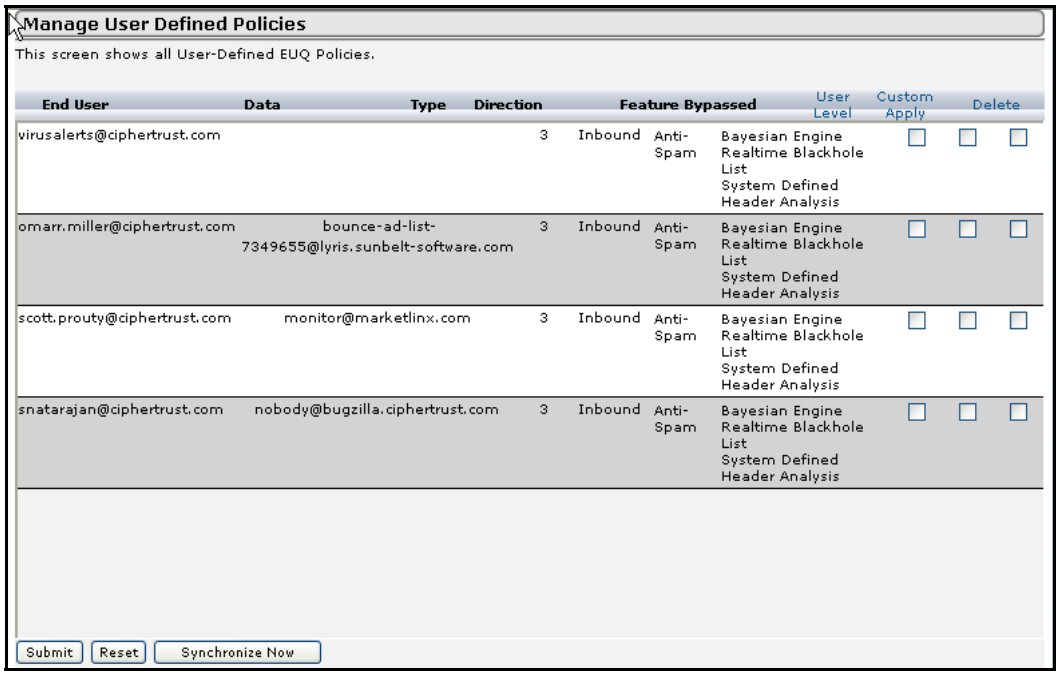
If the user selects one or more messages for whitelisting, the UI will send the message IDs and the user's email address to the Admin server. The email address is the value that is recorded in the `ct_eusr_qrelease` table. The Admin server validates the message and composes a record. If the user who requested the *rule* is the sender, the rule is created on each recipient or each recipient domain, and is applied as a *policy* to the user. If the user is the recipient, the rule is created on the sender or sending domain and applied to the user.

If the User Whitelist mode is set to manual, the server sets the status of the rule to -1. If the mode is set to automatic, the status is set to 0. Under the manual process, when the Administrator reviews the request and approves it, the status will be set to 0. This setting allows the records to be applied locally and to be synchronized as needed.

In automatic mode, the records are stored in the database and written to the whitelists directly. In manual mode, the records display in the GUI so they can be reviewed by the Administrator.

User-Defined EUQ Policies

Whitelist policies created as a result of end user requests are shown on the Manage User Defined Policies screen.



Field	Description
End User	This column shows the email address of the user who requested the whitelist policy
Data	This column displays the Email address or domain for the user or domain that is to be added to the whitelist.
Type	The whitelist type is based on the filter type set up when the whitelist is configured, email address or domain. The options are: • From Domain • To Domain • From Email • To Email
Direction	Inbound or Outbound direction.
Feature Bypassed	List of features from which the entity is to be whitelisted.
User Level	Checkbox indicating the whitelist rule is applied at the user level (for this end user only)
Custom Apply	Checkbox indicating the whitelist rule is applied to an entity other than the end user. **Note**: When a whitelist entry is custom applied, it will no longer show as a user-generated entry. It becomes an Administrator-generated entry.
Delete	Checkbox allowing deletion of whitelist entries.

Click **Submit** to save the information, or **Reset** to restore the screen to its condition after the last save.

The **Synchronize Now** command can be used when more than one IronMail appliance is configured in the *network*. Synchronizing assures that all whitelists on all applicable appliances are identical.

Virus Protection

Anti-Virus

If one or more anti-virus licenses have been purchased and installed on the IronMail appliance, it is capable of scanning all messages, whether incoming or outgoing, for viruses. By placing virus protection at the email gateway, administrators can have greater confidence that viruses will not enter their networks through email.

Administrators may purchase licenses for Authentium, McAfee and/or Sophos products. These anti-virus engines are seamlessly embedded within IronMail's queue architecture, providing robust protection against even the very newest viruses and worms. Virus definition or "identity" files can be automatically downloaded once an hour to ensure that IronMail is able to stop the most recent threats.

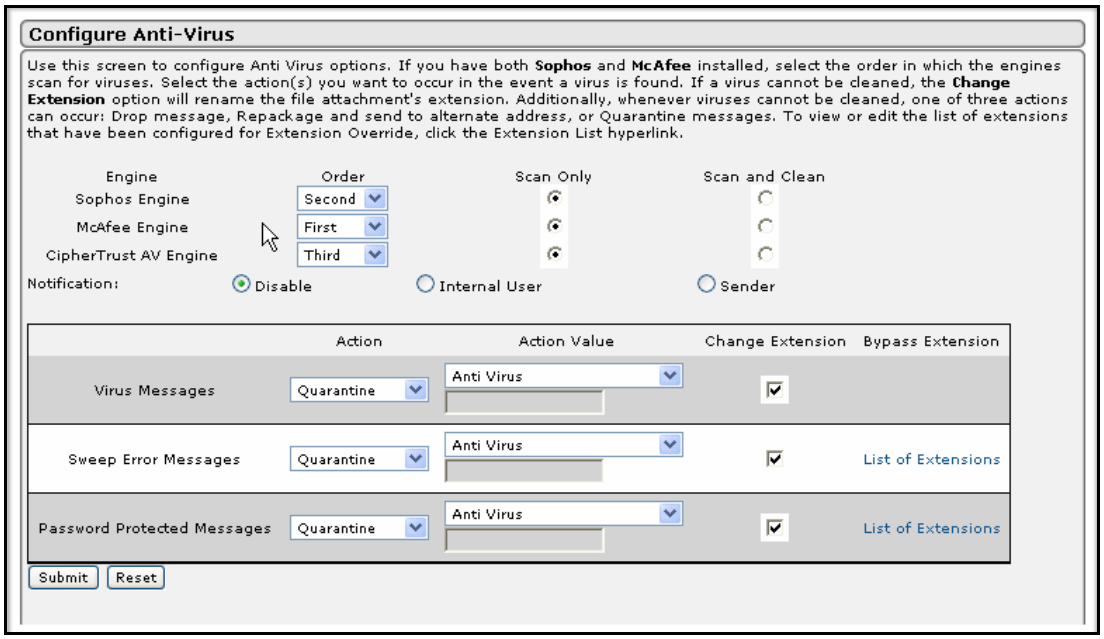
The IronMail Virus Engine can scan the contents within an attached zip file down to sixteen levels of zipping. If a virus is detected and it can be cleaned, this cleaning is performed. If it cannot be cleaned, action is taken on the entire zip part or the entire message. For example, the message may be quarantined or email delivery stopped.

When an anti-virus license expires, it disappears from the Web Administration interface and its functionality ceases on the midnight *before* the date of expiration. License renewals should be installed *prior* to license expiration. If a renewal license is installed *after* license expiration, administrators will have to manually re-configure anti-virus settings and place the Virus Scan Queue back into the Queue Order.

Configure Anti-Virus, Extension Override, Manual Anti-Virus Updates, Auto Anti-Virus Updates, and Current Anti-Virus Information hyperlinks in the left navigation frame allow navigation to the configuration options for IronMail's anti-virus protection.

Configure Anti-Virus

Basic configuration of IronMail's anti-virus capability is performed within the Configure Anti-Virus page. There are two components to IronMail's anti-virus strategy. The first component is to use the installed anti-virus engine to clean any viruses it detects—this is Authentium-, Sophos- and/or McAfee-dependent. The second component is IronMail-dependent—if neither engine can clean the virus, IronMail will perform an action specified in this Configure Anti-Virus page.


Configure Anti-Virus
Use this screen to configure Anti Virus options. If you have both Sophos and McAfee installed, select the order in which the engines scan for viruses. Select the action(s) you want to occur in the event a virus is found. If a virus cannot be cleaned, the Change Extension option will rename the file attachment's extension. Additionally, whenever viruses cannot be cleaned, one of three actions can occur: Drop message, Repackage and send to alternate address, or Quarantine messages. To view or edit the list of extensions that have been configured for Extension Override, click the Extension List hyperlink.
Engine
Order
Scan Only
Scan and Clean
Sophos Engine
Second
McAfee Engine
First
CipherTrust AV Engine
Third
Notification:
Disable
Internal User
Sender
Action
Action Value
Change Extension
Bypass Extension
Virus Messages
Quarantine
Anti Virus
Sweep Error Messages
Quarantine
Anti Virus
List of Extensions
Password Protected Messages
Quarantine
Anti Virus
List of Extensions
Submit
Reset

The screen provides the following configuration options:

Field	Description
Engine	The names of the installed anti-virus engines are displayed. Currently, IronMail issues licenses for Sophos, McAfee and Authentium anti-virus protection.
Order	The **Order** pick lists for each virus engine allow administrators to disable an anti-virus engine, or specify the running ordert. Administrators may use their own judgment when selecting an "order."
Scan Only / Scan and Clean	At the discretion of the administrator, each anti-virus engine may be configured either to "scan only" or "scan and clean." It is recommended that engines be set to "scan and clean."
Notification	Click the proper radio button to indicate how IronMail should issue notices regarding virus detection. Options are: • Disable - send no notices • Internal user - notify users within the *network* • Sender - notify the sender only, whether he is inside the network or not.
Table of Detectible Issues	***The lower portion of the screen identifies three types of detection issues and allows the Administrator to specify how they are to be treated.***
Error	The three types of issues are listed: Virus Messages, Sweep Error Messages, and Password Protected Messages.
Action	Each type of message has its own pick list. Options are: • For Virus Messages - Drop, Quarantine, or Forward • For Sweep Error Messages - Drop, Quarantine, Forward or Pass Through • For Password Protected Messages - Drop, Quarantine, Forward or Pass Through
Action Value	Enter any information related to the selected action, such as the email address to which messages should be forwarded, the number of days to hold messages in quarantine, etc. The name of the queue to which messages will be quarantined will also be selected.
Change Extension	Check the checkbox to enable IronMail to change the extension for any detected attachment that could not be cleaned..
Bypass Extension	For Sweep Error or Password Protected Messages, bypassing extensions is possible so the messages can be delivered. Each of the two message types has a List of Extensions hyperlink that allows Extension Override.

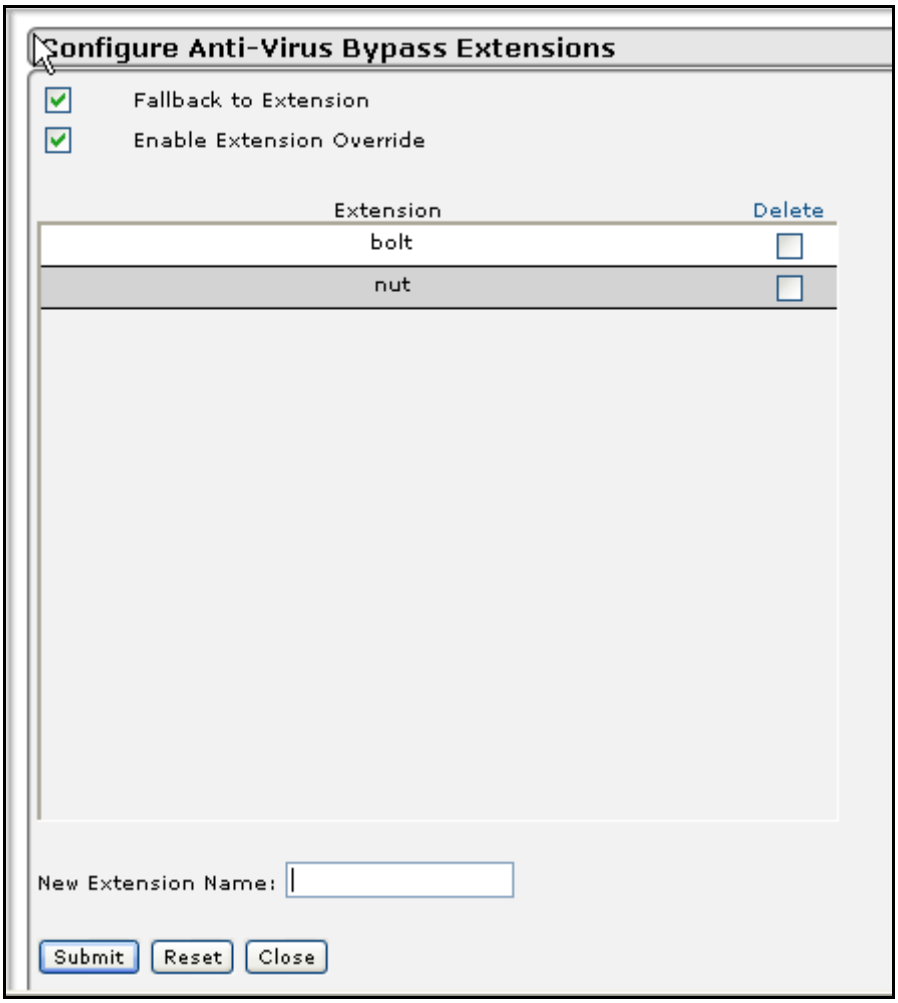
When you have entered or selected all the necessary entries, click **Submit**.

Extension Override

The Virus Queue is intended to scan incoming files (messages, etc.), detect any viruses that may be present, and clean the files if it can. If it cannot clean any particular file, IronMail will treat that file according to the policies and rules configured by the Administrator. If the Virus Queue cannot scan a file, it assumes that file contains a virus or viruses, and treats the file accordingly.

Sometimes the Virus Queue cannot scan a file because it is password protected, encrypted, or otherwise unreadable. To enable specific, protected files to pass through the Virus Queue, the Administrator may use the Extension Override functionality. This function allows you to create and

maintain lists of specific file extensions that are to be allowed to pass through the Virus Queue. Files with extensions that are not listed are subject to treatment like any other infected file.



Field	Description
Checkboxes	*Enable Extension Override* - Clicking this checkbox enables the override functionality for password protected files or sweep error files that are included in the list of password protected extensions. *Fallback to Extension* - Clicking this checkbox enables IronMail to use the Attachment Extension Method for identifying files when the Document Identification Method fails.
Extension	This column lists the extensions included in the Bypass Extension list..
Delete	*Delete* - Clicking this checkbox beside an extension will cause that extension to be eliminated from the list when you click **Submit**.
New Extension Name	Enter the new extension you wish to add. Do NOT included the initial period.

The Virus Queue proceeds through the scanning options in the following order.

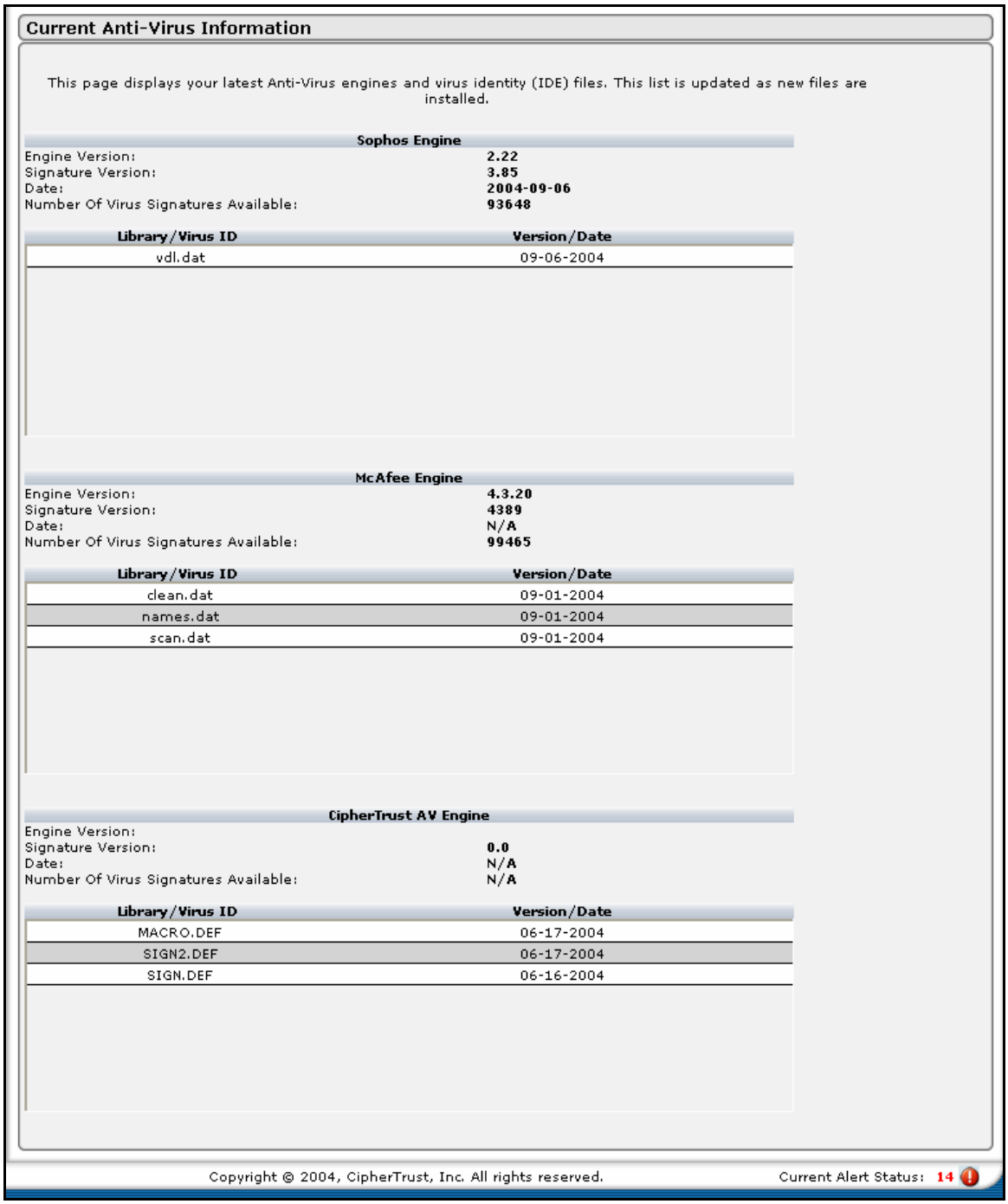
1. IronMail parses the original *MIME* message and identifies the file type.
2. IronMail scans the file using the Document Identification Method based on filters in the Content Extraction Queue. This option provides for the identification of approximately 295 file formats, based on the document without regard to any extensions.
3. If the first method fails, and if the Fallback to Attachment Extension Method checkbox has been checked, IronMail will use that method. The Attachment Extension Method is a part-level method that scans the extensions rather than the entire message.
4. If the second method fails or if it was not enabled, the Virus Queue will treat the file as a document type that is not included in the Extension Override lists.

Note: For messages with MIME parse failures, virus scanning is done on the message as a whole instead of scanning the message parts (body, attachments, etc.). For this reason the Extension Override functionality is not available for these messages. All Anti-Virus processing on MIME parsing failure messages and the action taken on these messages is logged in the Queue-Virus Scan log. If a message does fail MIME parsing, the Administrator can download the data from the message as a .dat file. The GUI will display a strong disclaimer warning the Administrator to use extreme caution because the message failed MIME parsing and may contain embedded viruses.

Current Anti-Virus Information

The Current Anti-Virus Information page allows administrators to verify that virus definition files for specific viruses-in-the-wild have been installed on the IronMail appliance. When, for example, an administrator learns that a virus is making its rounds around the Internet, he or she can navigate to this page to determine if a solution has been installed.

The Current Anti-Virus Information page contains a table of all virus identity (IDE) files installed since each vendor,s last cumulative “engine” was installed.



The table contains a separate section for each engine. The following information is available for each.

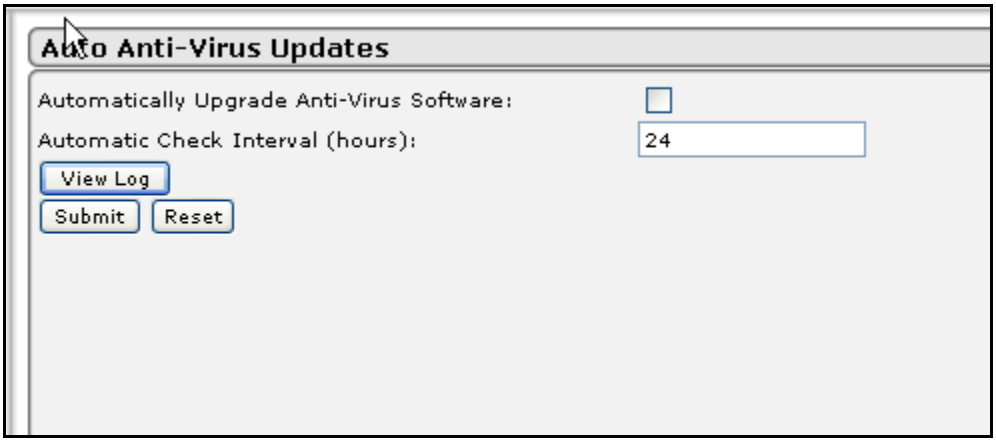
Field	Description
Engine Name	The name of the specific engine heads each section.
Engine Version	The engine version number appears in this field.
Signature Version	

Date	The date of the last update shows here.
Number of Virus Signatures Available	This field shows the total number of virus signatures included in the engine's protection for the *network*.
Library/Virus ID	The name or ID of a specific update for a virus or a library of viruses.
Version/Date	The date when this specific virus or library ID was updated.

The table of files is sorted in delivery date order with the most current updates at the top.

Auto Anti-Virus Updates

The preferred method for retrieving anti-virus file updates is to configure IronMail to automatically query CipherTrust's Update Server on a regular basis. If the Update Server reports that new files are available, IronMail will automatically download and install the files unattended in the background, without any administrative management of the appliance or interruption in mail flow.



Two options appear in the Automatic Anti-Virus Update Management page:

Automatically Upgrade Anti-Virus Software:	Select the **Automatically Upgrade Anti-Virus Software** check box and click **Submit** to enable auto-updating.
Automatic Check Interval (hours):	Enter a number, from 1 to 24, representing how frequently, in hours, IronMail should query the CipherTrust Update Server to see if new file updates are available.

A **View Log File** hyperlink at the bottom of the page records a history of all IronMail's queries and transactions with the Update Server. This is the same log viewed when clicking the **View Log File** hyperlink in Manual Anti-Virus Update Management page.

When auto updating is enabled, the Log File should look similar to the following:

++

virus Manager Starting Wed Oct 1 17:45:50 EDT 2003

virus Manager Starting Download of updates Wed Oct 1 17:45:50 EDT 2003

10012003
17:45:53:**********

10012003 17:45:53:Starting Update Process for Sophos Updates...

10012003 17:45:53:Reading configuration data...

10012003 17:45:53:Arguments passed sophos

10012003 17:45:53:Download Information from update.ciphertrust.net

10012003 17:45:54:Insert into Database Successful for SOPHOS-AV-372-ide20030725-07.07-87822f15a547781479c53aca6cc1fb5b

10012003 17:45:54:Insert into Database Successful for SOPHOS-AV-372-ide20030725-12.43-c8dfe4397441a6e8dd94182b6cb08884

virus Manager Completed Download of updates Wed Oct 1 17:45:55 EDT 2003

Start Updates for : < ide20030725-07.07 ide20030725-12.43 >

Completed Updates : < ide20030725-07.07 ide20030725-12.43>

++

10012003 17:45:55:Starting Update Process for McAfee Updates...

10012003 17:45:55:Reading configuration data...

10012003 17:45:55:Arguments passed mcafee

10012003 17:45:55:Download Information from update.ciphertrust.net

10012003 17:45:55:Insert into Database Successful for MCAFEE-4296-dat4296-ab12b28f75c053f6f301375f153bf81b

++

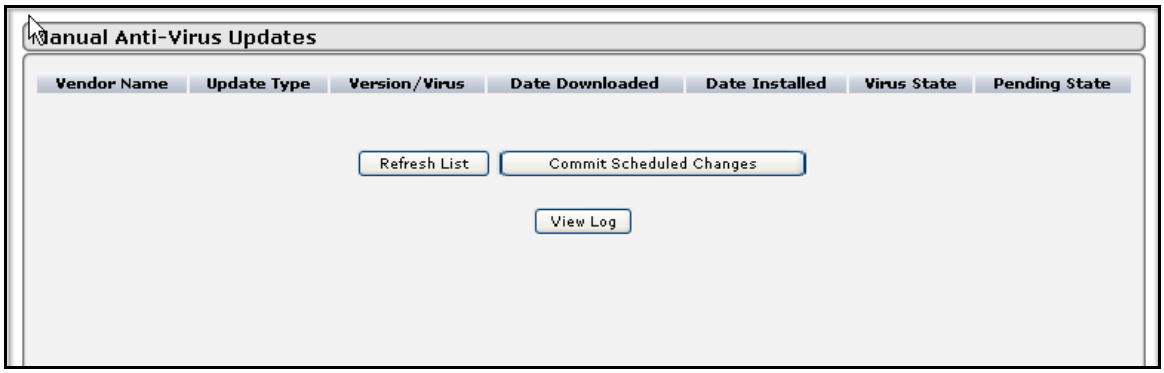
The *angle brackets* following "Start Updates" and "Completed Updates" indicate the files that were downloaded, updated, or inserted.

While neither Authentium, Sophos nor McAfee follow a routine schedule for delivering anti-virus updates (they are made available whenever virus solutions have been developed), they typically release new files at least once every 2-3 days, and sometimes several times a day. If more than four days transpire without receiving a virus update, contact CipherTrust Technical Support to confirm whether or not files are available. A good *rule* of thumb is to view the Anti-Virus Log File at least two to three times a week to ensure that IronMail is checking for anti-virus updates as expected.

Manual Anti-Virus Updates

CipherTrust checks for new virus definitions files from its anti-virus vendors every five minutes, and downloads them to its Update Server when they are available. In turn, IronMail administrators may configure their appliances to automatically check CipherTrust's Update Server for new anti-virus updates once an hour. If anti-virus files are available, they may be automatically downloaded and installed (if so configured—see Auto Anti-Virus Updates) in the background, without user input.

Administrators may elect to manually check for new virus definition files at any time by making a fresh query of CipherTrust's Update Server. If new files are reported to be available, administrators may manually download and install the new virus updates.



The Manual Anti-Virus Updates page contains a table, empty until IronMail queries the Update Server for the first time, reporting all anti-virus file updates that have been downloaded, installed, or are available to be downloaded. When the CipherTrust Update Server populates the table with file information, it sorts the table data in the order of update, from oldest file at the top to the newest file at the bottom of the table. When manually installing anti-virus file updates, install each file one at a time, in sequential order. Newer files may not be installed until all previous files have been installed. Note that IronMail allows administrators to *download* more than one file at a time. However, *installing* more than one file at a time is not recommended and can result in sequencing anomalies.

The table displays the following information:

Vendor Name	This column reports the name of the anti-virus vendor—either Sophos or McAfee.
Update Type	This column will display the type of update that each file represents. This is a vendor-specific identifier.
Version/Virus	This column reports the specific anti-virus engine or the name of the individual file definition. (Periodically the virus vendors will distribute a new "engine" that "rolls up" protection for all previously identified viruses. Until the next engine is released, the vendors release stand-alone identity files to provide protection on a virus-by-virus basis to protect against the most recently discovered viruses.
Date Downloaded	This column reports the date a file or engine was downloaded to the IronMail.
Date Installed	If a file or engine was installed, this column reports the date.
Virus State	This column reports the current state of an engine or file. The column will report one of three values: • **Available:** The file is currently available and ready to download. • **Downloaded:** The file has already been downloaded and is ready to be installed. • **Installed:** The file has been successfully installed. If the current state is **Available**, the administrator can change it to **Download**. If the current state is **Download**, the administrator can change it to **Delete** or **Install**. If the current state is **Installed**, the administrator cannot make any further changes.
Pending State	If the current state of any file has been changed from **Available** to **Downloaded**, or from **Downloaded** to **Install**, the new status is displayed in the Pending State column. The change is pending—not yet in effect—until **Commit Scheduled Change** is clicked.

The value in any column/row is also a hyperlink that opens a "file properties" window for that file within the main content frame of the Web Administration interface. Besides providing information about the file, a **Change State** pick list in that new window allows the administrator to select an action for the particular file. If the current state is **Available**, the administrator can change it to **Download**. If the current state is **Download**, the administrator can change it to ***Delete*** or **Install**. If the current state is **Installed**, the administrator cannot make any further changes.

After changing an individual file's status in the "file properties" window, click **Change State** to confirm that IronMail should make the change. The administrator is returned to the previous Manual Anti-Virus Updates page, where the change is now recorded in the **Pending State** column. (To return to the previous Manual Anti-Virus Updates page without making any changes, select "Cancel Change" from the **Change State** pick list and click **Change State**.) While multiple files may be deleted or downloaded simultaneously, never install or uninstall more than one file at a time. All anti-virus files must be installed sequentially.

After downloading or installing a file, click the View Log File hyperlink at the bottom of the page to view information about IronMail's transaction with the Update Server. Scroll to the bottom of the Log File to view the final status of the transaction. Note that this is the same log viewed when clicking the **View Log File** hyperlink in Auto Anti-Virus Update Management page. The log should display something similar to:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Generic Update Manager Starting Wed Jan 15 14:41:44 EST 2003
Updates to download:
Updates to install: ide20030115-14.00
Starting Install for update file ide20030115-14.00
Install complete for update file ide20030115-14.00
Insert Update to ironmail.domain.com, 9,ide20030115-14.00,, 20000
Updated ironmail with ide20030115-14.00-SOPHOS-AV-365
Updates to delete:
Updates to Uninstall:
Update Manager Finished Wed Jan 15 14:42:19 EST 2003
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

If the Log File reports that the installation was not successful, attempt to install the file again. If installation again fails, contact CipherTrust Technical Support.

Log File for Anti-Virus File Updating

The Log File is created the first time IronMail queries the Update Server, and its data is never deleted. Unlike many of IronMail's other files that are routinely deleted by the IronMail Cleanup Schedule, this log is not touched by the cleanup process. Note, therefore, that this log file can grow in size over the course of a year, and may take increasingly longer to load in a browser window as it becomes larger.

Capturing Spam

Anti-Spam Overview

IronMail offers a state-of-the-art anti-spam solution that blocks spam at the gateway. Because IronMail uses a suite of individual spam-blocking tools, spam entering the IronMail appliance isn't examined just once, but by all of the tools at IronMail's disposal. On the one hand, IronMail's anti-

spam strategy can be visualized as a funnel: a lot of spam enters the *network* at the wide opening of the funnel. The first of IronMail's spam-blocking tools can detect and stop a large percentage of that spam. Any spam making it past the first tool is then detected by the next spam-blocking tool. After that tool does its job, a little more spam may make its way through IronMail's spam-detecting processes. And each step reduces the numbers of spam messages that slip past, finally reducing the total number entering the network to a trickle of the original amount.

Another way of understanding how IronMail blocks spam is to realize that each of IronMail's separate spam-blocking tools is good at detecting particular kinds of spam. Because there is wide variety in how spam is constructed and delivered, a multi-tool strategy like this is able to cast a wide net, detecting more spam than single-approach anti-spam tools can.

Unlike many anti-spam solutions that offer only a "turn me on" option, IronMail lets administrators have total control, at a granular level, over how rigid or relaxed its anti-spam tools are as they individually react to suspected spam messages. Further, administrators may configure IronMail to take a "high level" approach to spam-detection by requiring more than one spam tool to think a message is spam before it is finally treated as such.

IronMail's spam-blocking tools examine messages within its Spam Queue.

Deny List, Reverse DNS, Realtime Blackhole List, Statistical Lookup Service, System Defined Header Analysis, User Defined Header Analysis, Enterprise Spam Profiler, User Spam Reporting, and Enterprise Spam Reporting hyperlinks provide access to IronMail's spam-blocking tools. In addition, a general Anti-Spam Strategy is also provided.

General Anti-Spam Strategy

Personnel Required

Anti-spam programs will differ somewhat depending on the size of the enterprise/organization and the goals of each anti-spam program. An aggressive program designed to stop the most spam will tend to generate more "false positives" than a less aggressive program.

The primary task of administrators when implementing IronMail's anti-spam tools is to develop "whitelists" of users and domains that generate legitimate messages that look like spam. That is, all of IronMail's anti-spam tools are quite effective at stopping spam. However, there are some legitimate mail applications that generate messages that have many characteristics of spam—such as e-newsletters that are mailed to thousands and tens of thousands of users. The challenge, then, is to let the spam tools do what they do well—detect spam—without stopping legitimate email. The IronMail approach, therefore is to monitor the messages that it thinks are spam, and whitelist the legitimate messages that were also detected as spam.

One of the primary ways to determine whether messages are really spam or "false positives" is to view the message header information in IronMail's quarantine queues. (Each of IronMail's spam-blocking tools can perform a variety of actions on messages they suspect are spam. One of the actions is "send to a quarantine queue"—a temporary holding area where administrators may actually view information about the message.) While spam will be easy to recognize in the quarantine queues, the "false positives" will be intermingled among them like diamonds in the terra firma out of which they are mined. Assuming that 20-40% of all email entering a domain may be spam, it is easy to see that, on a daily basis, administrators must sift through a lot of spam to pick out the legitimate messages that must be whitelisted and that in high-volume environments, several people might be required to sort through all the messages in the Quarantine Queue.

There is good news, though. On the one hand, each day as the whitelist grows, that many fewer false positives must be gleaned from among the suspected spam in the quarantine queues. And on the other hand, there are ways to minimize the need for manual inspection of messages for "false positives."

Approaches to Whitelisting

IronMail's anti-spam tools only block messages that they think are spam—either because the identical message has been delivered to thousands of users around the world, or because the message contains values in the message header that are typical of known spam. The solution to the problem of "false positives" is to whitelist all addresses and domains that generate email that looks like spam. There are three primary types of false positives:

- e-Newsletters such as Fantasy Football, Security Focus, SANS, etc. These are thought to be spam because of their sheer volume. The identical email is "seen in the wild" tens of thousands of times. These newsletters account for approximately 90% of all false positives.
- Listservers or newsgroups where users post questions and answers to each other. There are many business-critical newsgroups on the web that allow many users to respond to issues that others raise. However, the convergence of HTTP email and the way these web servers write the email header information makes the message header look forged or non-legitimate. These listserver messages account for approximately 7% of all false positives.
- Legitimate applications that send a message to large numbers of people and intentionally write non-standard header data. Some businesses use special software to send email announcements to large numbers of people, and the software does not write the RFC822 header information in the way typical mail client applications do, making those message look like spam. These applications are responsible for generating approximately 3% of all false positives.

All legitimate newsletters, listservers, and domains that generate legitimate mass mailings should be whitelisted so they are not stopped by IronMail's spam tools in the future. There are four approaches to whitelisting—with each requiring varying degrees of administrative effort—from almost no effort to considerable effort.

Almost No Effort:

Some organizations may wish to create a corporate *policy* that denies the receipt of all newsletters unless express permission is granted by an individual or group (e.g., Human Resources) within the organization. If this policy were in place, administrators would whitelist newsletters on a case-by-case basis and legitimately stop all others from being received, without fear of dropping needed emails. Generating a valid whitelist this way becomes an extremely easy task. This approach is successfully practiced in many enterprises.

Requires Just A Little Effort:

Some organizations believe that their users should be allowed to subscribe to many newsletters—whether business-related or for personal interest. In such a scenario, enterprises will send an email "blast" to all their employees notifying them that 1) they are introducing mechanisms to reduce the amount of spam entering their *network*; that 2) the anti-spam mechanisms will begin adding the words "SUSPECTED SPAM!!!" to the Subject line of any message they think are spam; 3) the anti-spam mechanisms will think that most newsletters are spam; and 4) users should, therefore, forward to the Email Administrator any newsletters they do not want blocked in the future. Enterprises allow IronMail to identify spam in this way for an entire month, allowing users to get used to the presence of the anti-spam software, and giving their users an entire month to let all their newsletters to be received. During this month, administrators begin creating and building their whitelist from the forwarded emails. At the conclusion of a month, administrators can confidently switch IronMail's actions from "Subject Re-Write" to another action, such as "Drop" or "Quarantine." This approach is successfully practiced in many enterprises.

Requires A Little More Effort:

Some organizations will set the action for IronMail's spam-blocking tools to "Log." Administrators will manually review the daily Policy Compliance Report's SPAM section. They will specifically

look for legitimate newsletters and email that were detected as suspected spam, and build their whitelist accordingly. While manually inspecting individual message header information in a report is relatively easy, it can still be tedious when tens of thousands of messages are logged each day. This approach does not allow administrators to actually view the body content of questionable newsletters. That is, some message Subject lines may look like those of legitimate newsletters, when in fact, they are really spam. Only the next approach allows administrators to view the actual message body to confirm that a message is really spam.

Requires Intensive Effort (for one week or more, then tapers off):

There are some organizations that prefer to keep their spam-blocking and "mail monitoring" practices hidden from the end users' view—they don't want individuals in their company to know they are examining their email. In this case, all newsletters will be allowed, but the whitelist that identifies them is generated solely by the email administrator. The administrator must configure IronMail to send suspected spam to a quarantine queue, where he or she—more likely, they—will visually pick out the legitimate newsletters from among the spam, and add them to a whitelist. As the whitelist grows each day, fewer newsletters end up in the quarantine queue, and it becomes easier to manually sift through its contents. After a period of one to four weeks, administrators may become confident that no more newsletters are being stopped, and so may configure IronMail to take an action other than "quarantine"—such as "drop." Again, this approach is successfully practiced in many enterprises.

Regardless of which approach to whitelisting is taken, administrators are strongly encouraged to develop their whitelist as much as possible before enabling IronMail's spam-blocking tools. Doing so reduces the number of false positives that must be identified from the very beginning. Creation and maintenance of whitelists is a *critically important factor* in an effective anti-spam strategy.

After all the anti-spam tools are in place, the question will inevitably arise, "Why is spam still getting into my network?" Some spam will not be detected because it is brand new—it has not circulated enough to be identified by spam-blocking servers. Other spam will enter the network because spammers have developed yet another novel way to defeat anti-spam tools. Fighting spam will be an ongoing battle, and the current "state-of-the-art" tools simply are not yet able to block 100% of spam.

How the Anti-Spam Tools Work Together:

Though IronMail provides a suite of individual spam-detecting tools, there are two basic methods for using them:

Tool-based Detection and Blocking: This method submits all incoming messages to any spam-blocking tools that have been enabled. Administrators specify the order in which the various tools examine a message. Messages are then processed sequentially through IronMail's anti-spam tools. Once a spam-blocking tool detects a spam message, that tool's "action" is performed, and all subsequent examination is terminated.

Confidence-based Detection and Blocking: This method submits all incoming messages to any spam-blocking tools that have been enabled. But instead of taking an action after the first tool identifies a message as spam, IronMail continues to examine the message with all remaining tools. After all the tools have finished their examination, IronMail generates a probability score—that is, the probability that the message is really spam, based on what each of the individual spam tools detected. An administrator-defined aggregate "confidence threshold" determines if the message is treated as spam, and if a specified action is taken.

Ordinarily, most administrators will enable Confidence-based Spam Detection and Blocking. Confidence-based detection increases the numbers of spam messages detected, while decreasing the number of false positives. Because all of IronMail's enabled spam-blocking tools are used—tools that could not formerly be trusted alone (e.g., reverse DNS and RBL lookups)—drop actions can now be used with confidence. That is, whereas an administrator might be confident enough only to send Statistical Lookup Service-detected messages to a quarantine queue, he or she may

now have confidence to delete messages that SLS, reverse DNS, and System Defined Header Analysis all thought were spam.

Confidence-based spam detection and blocking is enabled in *Anti-Spam > Enterprise Spam Profiler*. If Enterprise Spam Profiler is not enabled, IronMail defaults to tool-based spam detection and blocking.

Denying Mail

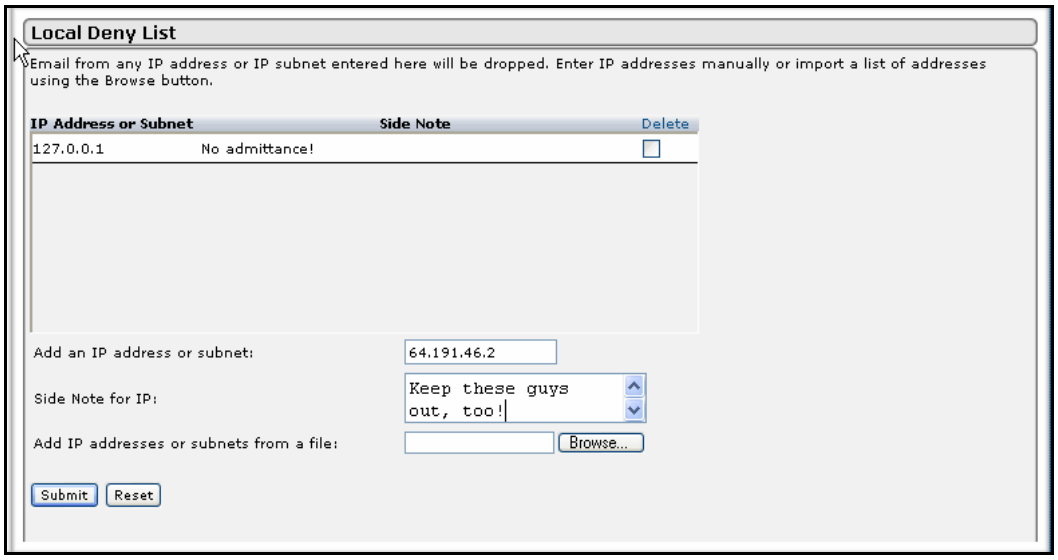
Deny Lists

IronMail displays three separate "deny lists." A "deny list" is a table of IP addresses that represent sources that are not allowed to send email to the *network*. The Deny Lists function at the level of IronMail's SMTPI Service. Whenever an external source attempts an SMTP connection, IronMail looks in each of these tables to see if the source IP is present. If the *IP address* is found in any Deny List, IronMail drops the connection, and the email is not accepted. Each of IronMail's three Deny Lists represents different ways the source IP addresses were identified. The Deny List hyperlink in the left navigation frame expands to offer Local Deny List, , RBL Drop List and Reverse DNS Drop List sub-menus.

Local Deny List

Before IronMail's SMTPI Service accepts a connection, it looks in the Local Deny List to see if the *IP address* is listed. If the IP address exists, the connection is dropped; if the IP address does not exist in this or the other two Drop Lists, IronMail accepts the connection.

The Local Deny List allows administrators to manually enter an IP address that should not be allowed to make a connection to IronMail. Whenever a spam message is able to get past IronMail's other spam-blocking tools, consider finding the message's IP address in the SMTPI Detailed Log and entering it in the Local Deny List. (See *Monitoring > Reports/Log Files > Detailed Logs* for a discussion on using IronMail's Detailed Logs.)

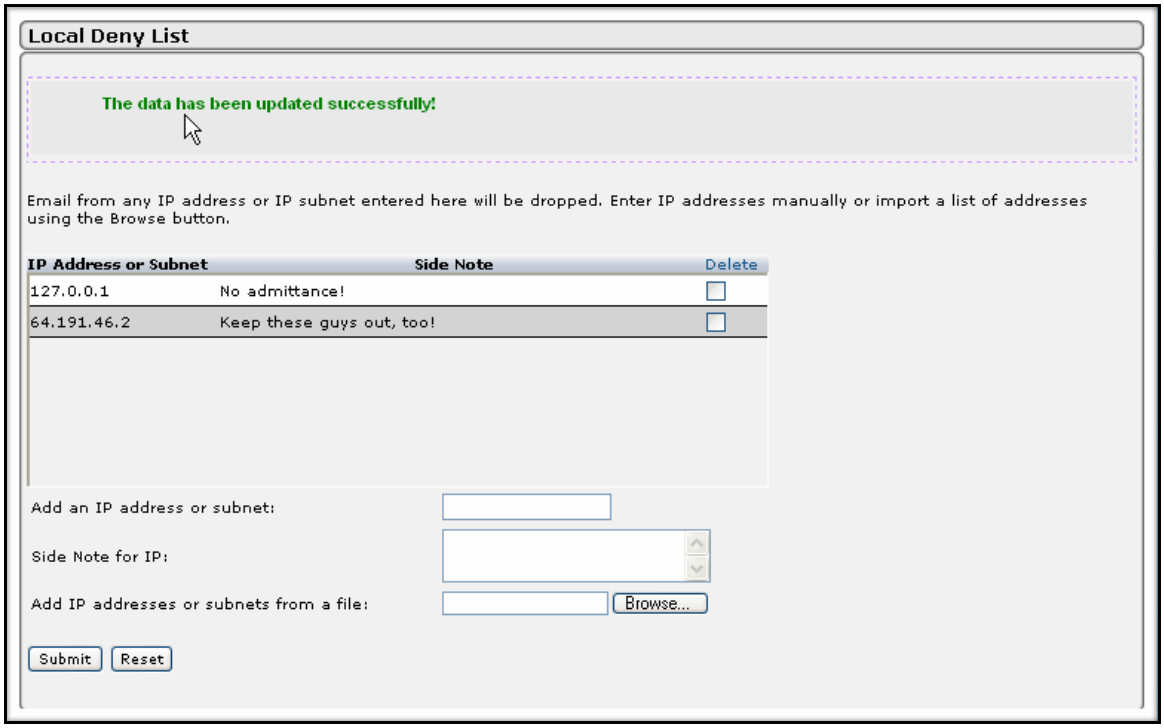

Local Deny List
Email from any IP address or IP subnet entered here will be dropped. Enter IP addresses manually or import a list of addresses using the Browse button.
IP Address or Subnet
Side Note
Delete
127.0.0.1
No admittance!
Add an IP address or subnet:
64.191.46.2
Side Note for IP:
Keep these guys out, too!
Add IP addresses or subnets from a file:
Browse...
Submit
Reset

The Local Deny List table provides the following information:

IP Address or Subnet	This column identifies IP addresses and subnets that have been manually entered by an IronMail administrator.
Side Note	This column reports a "friendly" description of the IP address.
Delete	Selecting an IP address' **Delete** check box and clicking **Submit** deletes the IP address from the table.

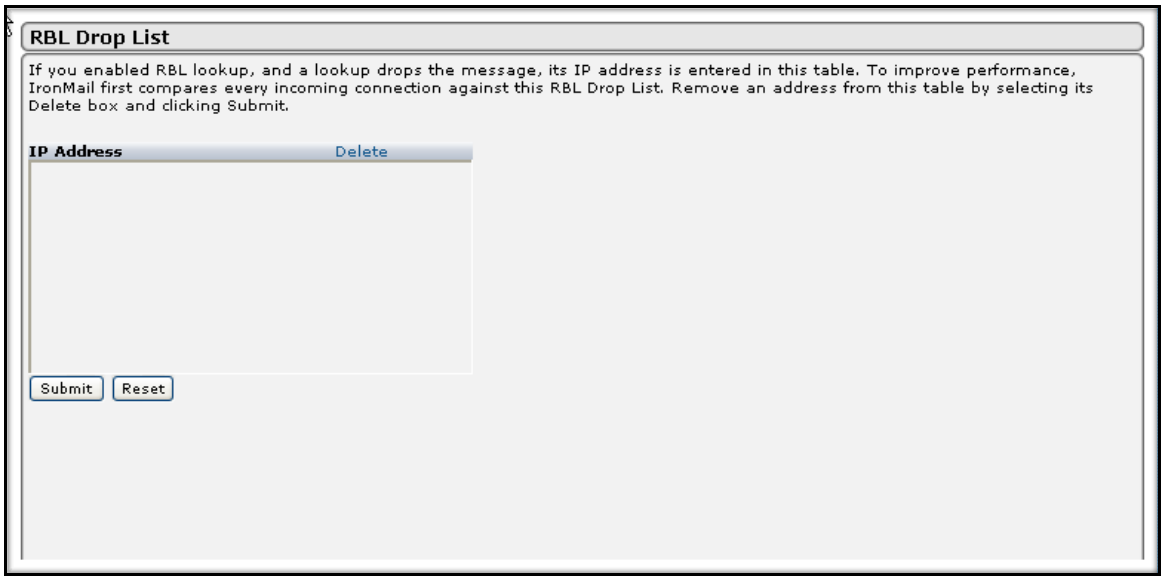
Adding Addresses	***Three input fields below the Local Deny List table allow administrators to add IP addresses to the table.***
Add an IP address or subnet	Enter an IP address. Subnets may be entered, but only entire Class A, B, or C subnets are allowed. Enter only one IP address or subnet at a time.
Side Note for IP	Enter any text that will help other users understand why the particular IP address has been added to the Local Deny List. A side note is not required when entering an IP address. However, a side note for an address cannot be added later. Therefore, to ensure that a side note accompanies an IP address, ensure that one is created when the IP address is first submitted to the Local Deny List table.
Add IP addresses from file	If a list of IP addresses that should not be allowed to connect to IronMail already exists in a plain ASCII text file, click **Browse** to navigate to the file. Note that each IP address and side note in the text file must be separated from the others with a carriage return, and the IP address and the side note must be separated from each other by the pipe ("|") symbol. When importing IP addresses from a text file, side notes are not required. (See the Appendix chapter for a complete discussion of formatting requirements when importing text files into IronMail.)

Click **Submit** after entering data in the input fields. The Local Deny List is updated.


Local Deny List
The data has been updated successfully!
Email from any IP address or IP subnet entered here will be dropped. Enter IP addresses manually or import a list of addresses using the Browse button.
IP Address or Subnet
Side Note
Delete
127.0.0.1
No admittance!
64.191.46.2
Keep these guys out, too!
Add an IP address or subnet:
Side Note for IP:
Add IP addresses or subnets from a file:
Browse...
Submit
Reset

RBL Deny List

Before IronMail's SMTPI Service accepts a connection, it looks in the RBL Drop List to see if the *IP address* is listed. If the IP address exists, the connection is dropped; if the IP address does not exist in this or the other two Drop Lists, IronMail accepts the connection. The RBL Drop List is automatically generated by IronMail if Realtime Blackhole List (RBL) is enabled as an anti-spam tool and its action is configured to "drop." The table of IP addresses is populated with the IP address of any source that tries to connect to IronMail, but whose connection IronMail dropped because an RBL query reported that the address was a known spammer.


RBL Drop List
If you enabled RBL lookup, and a lookup drops the message, its IP address is entered in this table. To improve performance, IronMail first compares every incoming connection against this RBL Drop List. Remove an address from this table by selecting its Delete box and clicking Submit.
IP Address
Delete
Submit
Reset

The RBL Drop List table provides the following information:

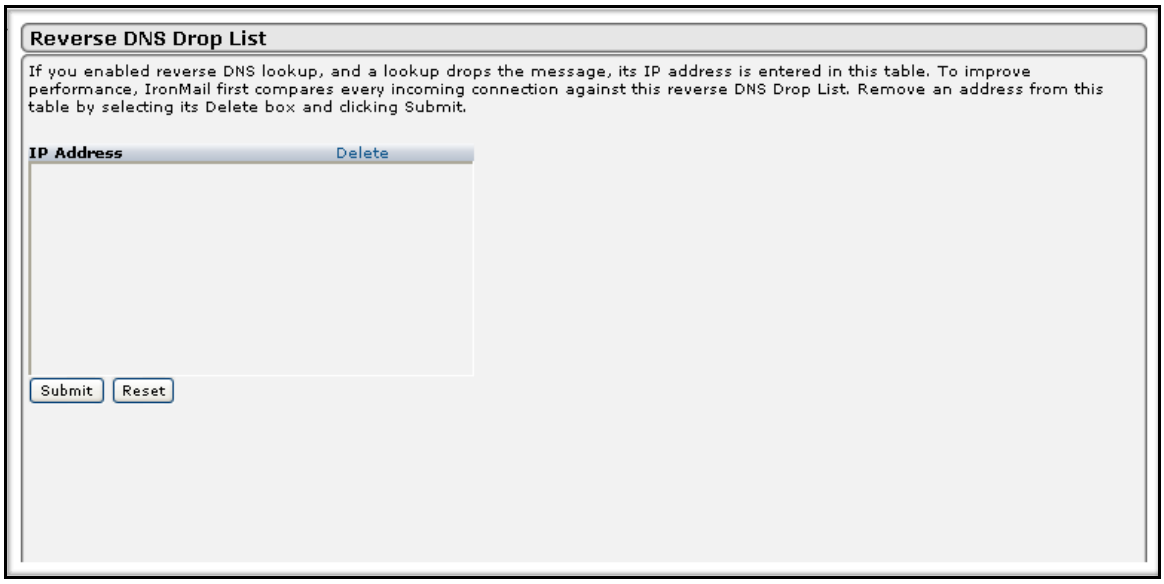
IP Address	This column identifies IP addresses of any source whose connection was dropped because an RBL lookup determined the source was a spammer. (If IronMail's RBL anti-spam "action" was not configured to Drop—e.g., configured, instead, to Quarantine—the source IP would not be added to this table.)
Delete	Selecting an IP address' **Delete** check box and clicking **Submit** deletes the IP address from the table.

The RBL Drop List grows over time (if RBL is enabled with a Drop action), and its data is not deleted by IronMail's Cleanup Schedule (*Administration > Cleanup Schedule*).

Note that RBL services have been known to black list legitimate domains for a variety of reasons. If expected email from a domain suddenly stops being received, check that the domain's IP address has not inadvertently ended up on this RBL Drop List. If so, select its **Delete** check box and delete it from the table. Consider placing that IP address on IronMail's whitelist so that future instances of an incorrect RBL blacklisting do not occur. Because the RBL Drop List is not automatically updated, the resulting build up of black list entries can affect IronMail performance. After the RBL Drop List grows over time, it is a good idea to remove entries from the RBL Drop List and start with an empty list and rebuild it (if RBL is enabled as an anti-spam tool and its action is configured to "Drop"). This also helps to avoid the black listing of legitimate domains.

Reverse DNS Deny List

Before IronMail's SMTPI Service accepts a connection, it looks in the Reverse DNS Drop List to see if the IP address is listed. If the IP address exists, the connection is dropped; if the IP address does not exist in this or the other two Drop Lists, IronMail accepts the connection. The Reverse DNS Drop List is automatically generated by IronMail if Reverse DNS is enabled as an anti-spam tool and its action is configured to "Drop." The table of IP addresses is populated with the IP address of any source that tries to connect to IronMail, but whose connection IronMail dropped because a reverse DNS query could not validate the *host name*.


Reverse DNS Drop List
If you enabled reverse DNS lookup, and a lookup drops the message, its IP address is entered in this table. To improve performance, IronMail first compares every incoming connection against this reverse DNS Drop List. Remove an address from this table by selecting its Delete box and clicking Submit.
IP Address
Delete
Submit
Reset

The Reverse DNS Drop List table provides the following information:

IP Address	This column identifies IP addresses of any source whose connection was dropped because a reverse DNS lookup failed. (If IronMail's Reverse DNS anti-spam "action" was not configured to Drop—e.g., configured, instead, to Quarantine—the source IP would not be added to this table.)
Delete	Selecting an IP address' Delete check box and clicking Submit deletes the *IP address* from the table.

The Reverse DNS Drop List grows over time (if Reverse DNS is enabled with a Drop action), and its data is not deleted by IronMail's Cleanup Schedule (Administration > Cleanup Schedule). In addition, because the Reverse DNS Drop List is not automatically updated, the build up of entries can affect IronMail performance. It is a good idea to remove entries from the Reverse DNS Drop List and start with an empty Reverse DNS Drop List and let the list become automatically regenerated if Reverse DNS is enabled as an anti-spam tool and its action is configured to "Drop."

Note that while Reverse DNS used to be an effective tool to identify spammers, it has recently become less so. Increasingly, domains are both incorrectly and intentionally not configuring their servers for reverse DNS. Therefore, reverse DNS queries may populate this Drop List with many legitimate IP addresses, and frequent trips here may be required to delete valid IP addresses. Administrators should be extremely cautious when configuring IronMail's reverse DNS to drop connections.

Reverse DNS

Reverse DNS

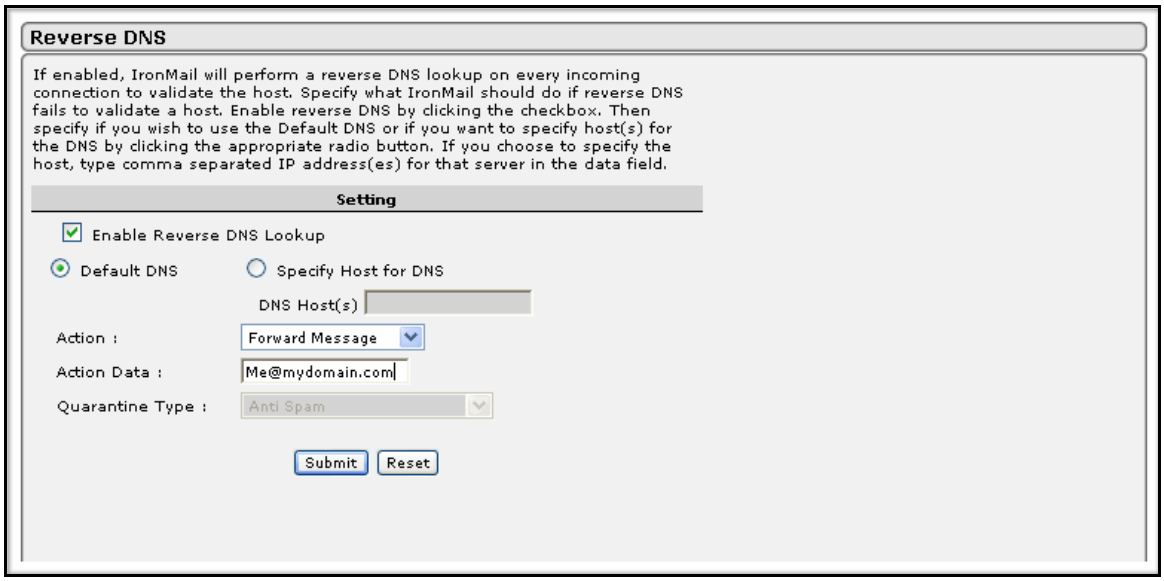
Whereas a normal DNS lookup is used to resolve a *host name* to an IP address, a reverse DNS lookup is used to resolve a message sender's IP address to a valid host name.

Normal DNS: thispc.thisdomain.com = 10.20.1.210

Reverse DNS: 10.20.1.111 = thatpc.thatdomain.com

If a reverse DNS entry is not present in DNS, it may indicate that the sender is a spammer. Note that IronMail only queries the *DNS server* for the presence of a reverse DNS entry. It does not resolve the *IP address* to the host name. Also note that if IronMail is behind some versions of proxy-type firewalls, reverse DNS will not function correctly. The *firewall* will present *its* IP address to the DNS server instead of the address of the sending host.

Due caution should be used when enabling IronMail's Reverse DNS lookup. While reverse DNS used to be effective at detecting spammers, domains are increasingly incorrectly or intentionally not configuring their servers for reverse DNS. Therefore, reverse DNS queries may incorrectly consider legitimate email as spam. Administrators may be advised to set the Reverse DNS action to Log or Quarantine instead of Drop or Subject rewrite. After monitoring the results of reverse DNS queries, administrators may decide not to implement this tool, *unless* confidence-based spam detection and blocking is being implemented.


Reverse DNS
If enabled, IronMail will perform a reverse DNS lookup on every incoming connection to validate the host. Specify what IronMail should do if reverse DNS fails to validate a host. Enable reverse DNS by clicking the checkbox. Then specify if you wish to use the Default DNS or if you want to specify host(s) for the DNS by clicking the appropriate radio button. If you choose to specify the host, type comma separated IP address(es) for that server in the data field.
Setting
Enable Reverse DNS Lookup
Default DNS
Specify Host for DNS
DNS Host(s)
Action :
Forward Message
Action Data :
Me@mydomain.com
Quarantine Type :
Anti Spam
Submit
Reset

The Reverse DNS page requests the following input:

Enable Reverse DNS lookup	Select the **Enable Reverse DNS** lookup check box to turn on this anti-spam tool. When enabled, IronMail will perform a reverse DNS query for every message that does not originate from a domain identified in *Mail-Firewall > Mail Routing > Domain-based*.
Default DNS	Click this radio button if you want to use the default host for your DNS.
Specify Host for DNS	Click the radio button to specify the host or hosts you want to use, then enter the IP address or fully qualified host name of one or more RBL servers in the associated data field. Multiple IP addresses and host names must be separated from each other with commas. Do not enter spaces between the commas and the beginning of each IP address or host name.

Action	IronMail can perform one of 8 actions if a message source does not have a reverse DNS entry in DNS. Select an action from the **Action pick** list. Note that some actions require qualifying information to be entered in the **Action Data** field below. • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the **Action Data** input field below. For example, messages that fail a reverse DNS lookup can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the **Action Data** input field immediately below. • **Drop message:** IronMail will drop the entire message. Also the IP address will be added to the RDNS drop list for any future messages. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the **Action Data** field. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Data** field indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Log:** IronMail will deliver the message, but record in its SPAMQ Detailed Log that the message failed a reverse DNS lookup. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** This is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the spam *policy* definitions.

Action Data	Some actions require qualifying information. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not enter spaces between commas and subsequent email addresses.) • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not enter spaces between commas and subsequent email addresses.) • **Add Header:** A text string is required and must follow the RFC822 *protocol* rules for custom headers. The custom header format is: "**headername:headervalue**" where **headername** is an arbitrary name for the custom header, and **headervalue** is an arbitrary text string to display in the header. A sample custom header might be: "**HA-SPAM: 50**" ("**HA-SPAM**" is shorthand for "Header Analysis detected this message as SPAM," and "**50**" represents the policy's threshold. The string to the right of the colon—the header value—cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** This action requires the host name and address of the dedicated IronMail appliance to which messages will be re-routed.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** pick list is enabled. A Queue must be specified.

Click **Submit** to save the user input.

Administrators may look in the detailed "SpamQ" Log to see the results of reverse DNS lookups. (Note that the Anti-Spam Queue's Log Level must be set to "6"—*Queue Manager > Configure Queues > Queue-Anti-Spam > "Log Level*.") See Understanding Detailed Logs for information on viewing message details in the SpamQ log.

RDNS and ESP

Reverse DNS contributes to the overall ESP Profile in a simple way. RDNS returns a score of 100 if no PTR record was found for the domain being processed, and a score of 0 if a PTR record was found for the domain.

Values	No PTR record found: 100 (this is potentially a spam message) PTR record found: 0 (this is likely to be a legitimate message) Confidence value: a pre-configured percentage
Formula	ESP Contribution = RDNS value X Confidence %
Example	ESP Contribution = 100 X 20% = 20 points

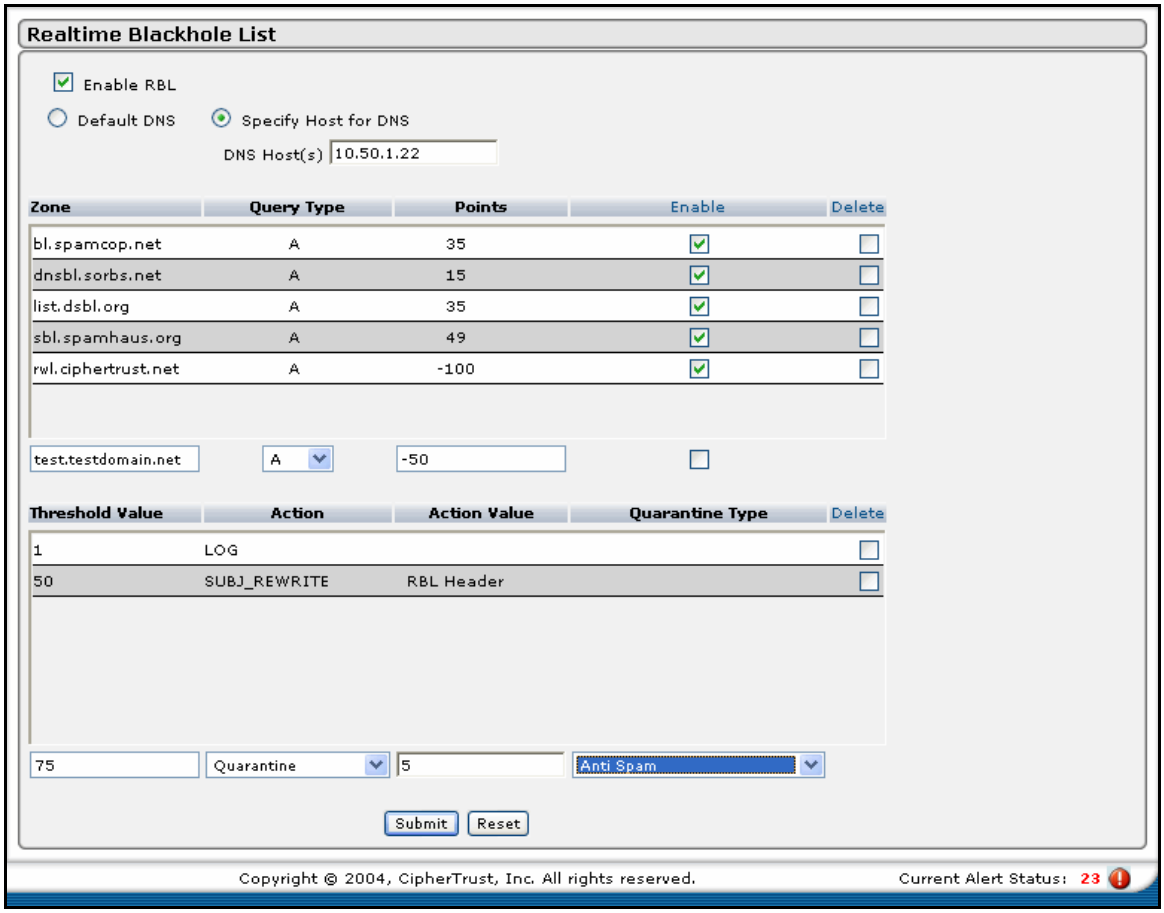
Blackhole Lists

Realtime Blackhole List

IronMail performs an RBL query on each message that does not originate from a domain listed in the Domain-Based Routing table. If enabled, IronMail performs a query of one or more RBL services. If the RBL service reports that the message-sender's *IP address* is on its list as a known spammer, IronMail will take the action specified on this page.

By default, IronMail performs its RBL lookup only on the host that is connected to it. This is the most effective configuration so long as IronMail is positioned before the gateway of the *network*. In those rare instances when IronMail is positioned after the gateway, it can be configured by CipherTrust Support to perform its query against the IP address in the message header. CipherTrust recommends that the default configuration be used in all cases where IronMail is before the gateway.

Note: Due caution should be used when enabling IronMail's RBL lookup. Legitimate businesses sometimes find themselves—for a variety of reasons—on an RBL list. While some administrators are more confidant in RBL services and comfortably select a Drop action for messages reported as spam, others are more cautious and quarantine RBL-suspected spam.



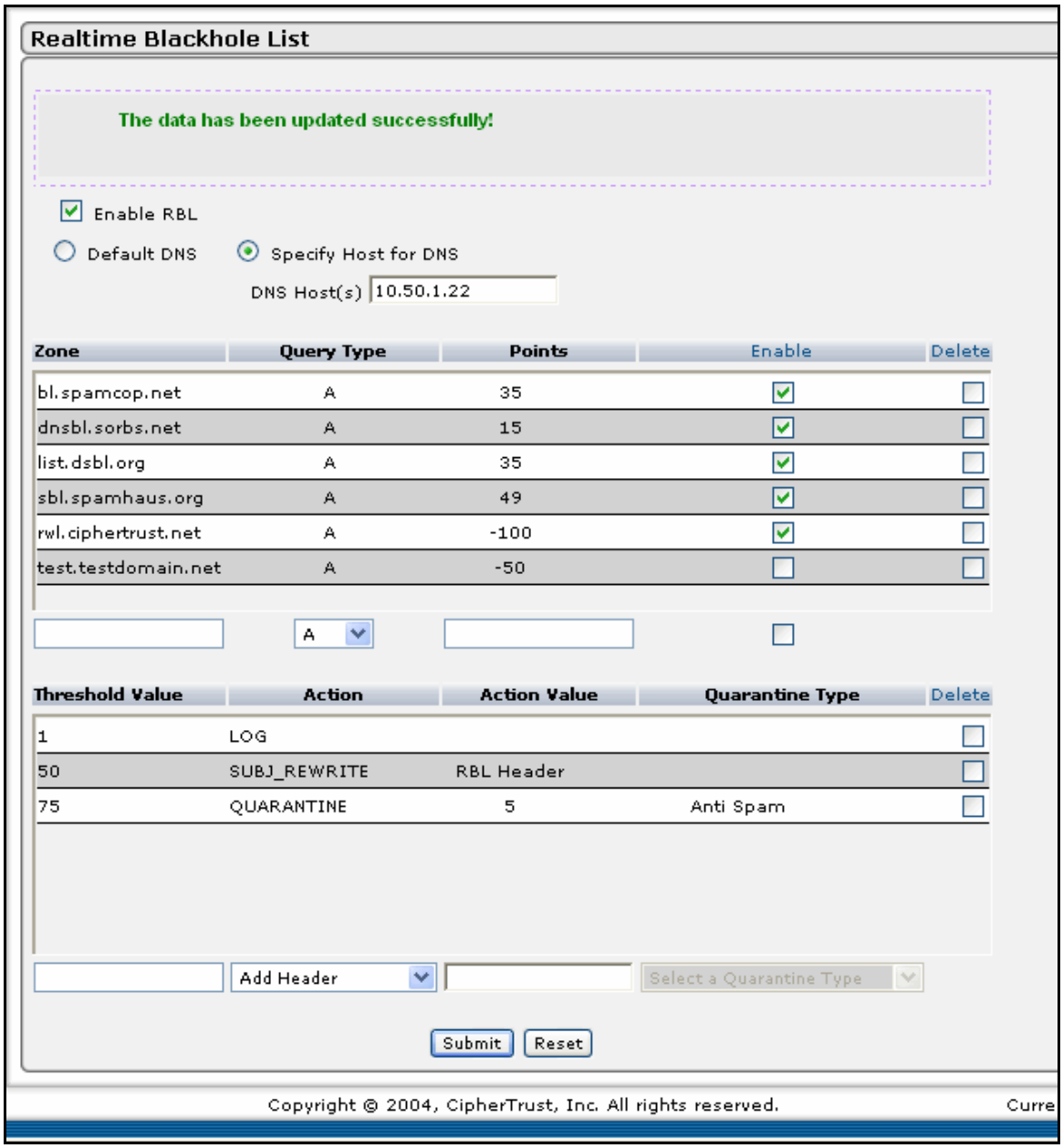
The Realtime Blackhole List page requests the following input:

Enable RBL	Select the **Enable RBL** lookup check box to turn on this anti-spam tool. When enabled, IronMail will perform an RBL query for every message that does not originate from a domain listed in its domain-based routing table (*Mail-Firewall > Mail Routing > Domain-based*).
Default DNS	Click this radio button if you want to use the default host for your DNS.
Specify Host for DNS	Click the radio button to specify the host or hosts you want to use, then enter the IP address or fully qualified *host name* of one or more RBL servers in the **DNS Host(s)** data field. Multiple IP addresses and host names must be separated from each other with commas. (Do not enter spaces between the commas and the beginning of each IP address or host name.) When multiple RBL servers are entered, IronMail queries each server in turn until one returns a positive result (i.e. the source IP is on its RBL list), after which no further queries are performed. Up to 100 bytes of data may be entered in the RBL Hosts input field.
Upper Table	
Zone	This field contains the list of RBL zones for which filters have been configured.
Query Type	This column displays the type of query to be run. The choices are "A" and "TXT" searches; IronMail will search the record type specified.
Points	This column displays the points assigned to each Zone.
Enable	If this check box is checked, RBL for the particular zone is enabled. If you wish to disable that zone, click the check box to remove the existing check. The zone will be disabled when you press **Submit**.
Delete	If you wish to delete the zone, check the Delete check box. When you press **Submit**, the zone will be deleted.
New Zones	The "Add" line displays the entry fields, etc., for configuring new filters. • In the first box, enter the host name or IP address for the zone • In the drop-down list box, select the query type you prefer • Enter the point score for this zone (positive or negative) in the data field. • Select the check box if you want to enable the zone as soon as it is submitted. The new zone will be added when you click **Submit**. This feature allows the Administrator to enable DNS whitelisting by providing the capability to configure DNS zones that contribute negative numbers to the final ESP score for the message, reducing the likelihood that the message will be treated as spam. DNS whitelisting allows legitimate email senders to have their IP addresses whitelisted to avoid accidentally being blocked or quarantined. The ability to contribute negative ESP scores can ensure this.
Lower Table	
Threshold Value	This column shows the threshold values for filters that have already been configured.

Action	IronMail can perform one of 8 actions if a filter reports that the source address is that of a known or suspected spamme, as shown below. This column shows the actions that have been selected. Note that some actions require qualifying information to be entered in the **Action Data** field immediately below. • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value input field below. For example, messages from the specified user, or with the specified Subject, can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the Action Data input field immediately below. • **Drop message:** IronMail will drop the entire message. If drop is selected, the IP address is added to the RBL Drop List. Subsequent delivery attempts from that IP will be dropped in the SMTP proxy. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Data** field indicating how many days the message remains in the queue before being delivered out of the IronMail appliance. • **Log:** IronMail will deliver the message, but record in its SpamQ Detailed Log that the message matched a Mail Monitoring *rule*. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** Re-route is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the spam *policy* definitions.

Action Value	Some actions require qualifying information, shown in the **Action Data** column:. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not insert spaces between commas and subsequent email addresses.) • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not insert spaces between commas and subsequent email addresses.) • **Add Header:** A text string is required and must follow the RFC822 *protocol* rules for custom headers. The custom header format is: **"X-headername:headervalue"** where headername is an arbitrary name for the custom header, and headervalue is an arbitrary text string to display in the header. A sample custom header might be: "X-HA-SPAM: 50" ("X-" represents "custom," "HA-SPAM" is shorthand for "Header Analysis detected this message as SPAM," and "50" represents the policy's threshold. The header value string following the colon cannot be longer than fifteen characters, and the custom header *name* may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** This option requires a host name and address for the dedicated IronMail appliance to which messages are to be re-routed.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** the associated queue is displayed in this column.
Delete	If you wish to delete the filter, check the Delete check box. When you press **Submit**, the zone will be deleted.
Add New Action	The "Add" line displays the entry fields, etc., for configuring new filters. • In the first box, enter a number to represent the threshold at which you want the filter to trigger action. • In the drop-down list box, select the Action you want to associate with this threshold. • In the adjacent data field, enter the action value, if applicable, for the action you have selected. • If the action is "Quarantine," select the queue to which you want messages quarantined by this filter. The new filter will be added when you click **Submit**.

Click **Submit** to save the user input.



Administrators may look in the Detailed SPAMQ Log to see which RBL server reported that the sending IP address was a spammer. (Note that the Anti-Spam Queue's Log Level must be set to "6"—*Queue Manager > Configure Queues > Queue-Anti-Spam*—to record this level of detail.) See Understanding Detailed Logs for information on viewing message details in the SpamQ log.

Multiple Blacklists

Multiple RBL servers are allowed; IronMail accounts for each one separately, submitting all the IPs from the messages to each blacklist in succession. Each RBL is assigned its own confidence level, and can contribute to the ESP Profile. Different RBLs may have different confidence levels and may be configured for different actions for each threshold.

Up to ten (10) RBL servers may be configured, but CipherTrust recommends that no more than two (2) be enabled to assure maximum performance levels.

RBL and ESP

Realtime Blackhole List functionality returns an absolute point value to ESP, based on the point value that has been associated with each configured zone in RBL. Any realtime Whitelist configured with a negative point value will return that negative value to ESP.

Values	Specific point values assigned to each zone in the list: positive numbers for blacklist entries, and negative numbers for whitelist entries.
Formula	ESP Contribution = Sum of all matched RBL zone points.
Example	bl.spamcop.net 10 points dnsbl.sorbs.net 15 points ct-rwl.ciphertrust.com -20 points If the connecting *IP address* was in the first and second RBL lists, the ESP contribution would be 25 points (10 pts + 15 pts). If the connecting IP address was maintained in the third list, the ESP contribution would be -20 points.

TrustedSource

TrustedSource™ is a reputation-based authentication tool that is designed to weed out spam by identifying "good" senders. It attempts to identify legitimate email by rating the reputation of the sender, which it deteremines by monitoring the 7.5 million enterprise email boxes protected by IronMail. Unlike the reputation-based blacklists that identify spammers based on their sending behavior (e.g., mass mailings), and then reject their messages, TrustedSource identifies mail coming from what it determines to be valid or reputable sources and gives that mail a positive rating.

IronMail keeps the TrustedSource database pure by not allowing any email senders to beg or buy their way onto the list. And, unlike other whitelists, TrustedSource's validation of any message does not prevent IronMail from passing it through all other enabled spam filters. TrustedSource is not a bypass list. IronMail weighs the rating provided by TrustedSource against all other filter ratings before it considers the message valid.

The TrustedSource list is controlled and maintained by CipherTrust. However, anyone may request to be added to the list or to have a particular *IP address* added by sending an email to rwl-feedback@ciphertrust.com.

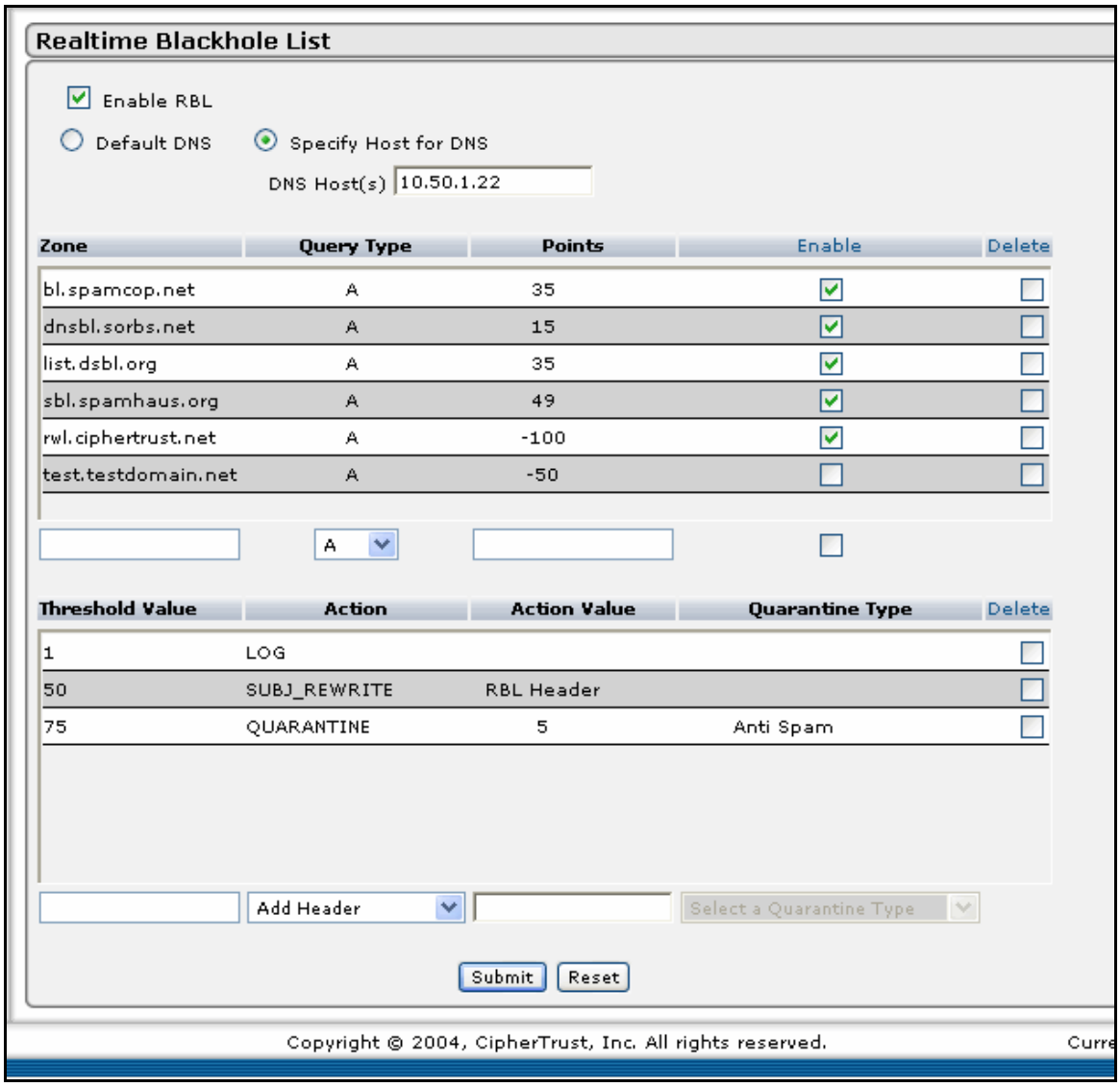
TrustedSource works in the Enterprise Spam Profiler (ESP) as a Realtime Blackhole List server, but instead of contributing positive numbers to the potential spam score, it contributes negative numbers that reduce that score.

Configuring TrustedSource

You may configure TrustedSource in either of two ways:

- you can install Threat Response Update (TRU) version 5 or higher, or
- you can configure it manually.

To configure manually, go to Anti-Spam > Realtime Blackhole List and add rwl.ciphertrust.net with a Query type of "A" and a *negative* point value.



If your IronMail appliance is not the first hop into your system, ***you cannot use TrustedSource***, because:

- the last hop in your message headers will always be the trusted IP, and
- if you allow the RBL query to check all routing IPs, you will discover that spammers bury valid IPs in their headers to get around detection.

Statistical Detection

Statistical Lookup Service

CipherTrust maintains a "trusted ring" of partners who participate in a collaborative effort to identify spam. The trusted partners all submit a hash of every email they receive—a numeric representation of an email's body—to CipherTrust. CipherTrust's Statistical Lookup Service (SLS) server maintains a count of how many times each hash has been reported to it. When IronMail administrators enable the Statistical Lookup Service anti-spam tool, they become members of the trusted ring of partners.

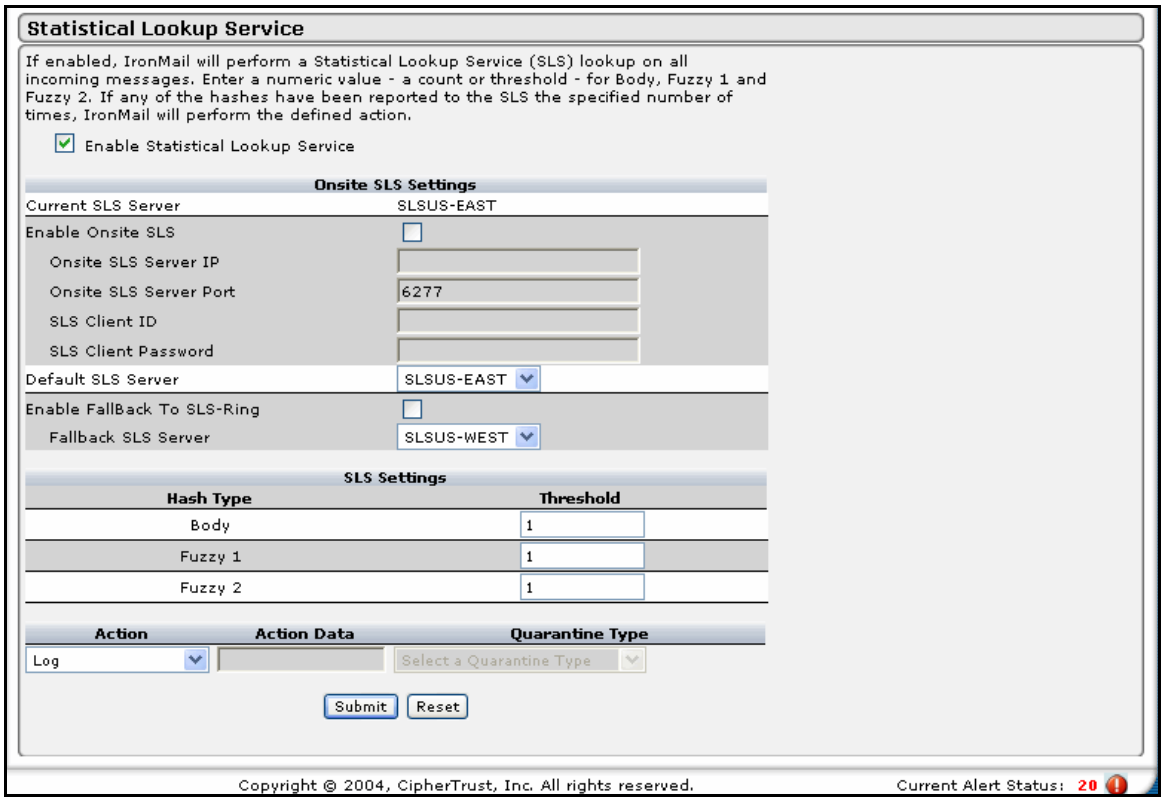
Removing newsletters from the equation, SLS is a highly accurate spam-detector—with the lowest percentage of false positives of any spam-blocking tool available. Depending on how the enterprise

wishes to handle newsletters, SLS may be safely set to drop messages. Prudence might propose that a period of testing be performed first, however, with SLS quarantining messages for a period of time. Alternately, SLS can quarantine messages, and if a "quarantine value" of "0" is provided the messages will automatically be deleted on IronMail's next cleanup cycle.

While administrators will enter "thresholds" suggesting that sheer volume correlates directly with spam, the thresholds are not meant to suggest that SLS will begin making false positives if the threshold is too low. (CipherTrust uses thresholds of "10" on the IronMails it uses in its own email system, and has only experienced false positives on newsletters.) Non-spam email is so genuinely unique that it is highly unlikely that SLS will create a hash that is identical to another legitimate message. Administrators do not have to be cautious in setting SLS thresholds—for example, starting with threshold values of 200 or higher. The default threshold values of 10, 25, 25 are quite acceptable.

IronMail will create *three hashes of each incoming message* and submit them to the SLS server. If the SLS server reports that the hash has been seen more times than indicated as the "threshold," the specified action is taken. The Body hash is a hash of the body of the email—a numeric representation of the message body as it exactly is. Because spam applications frequently alter each message body slightly—e.g., inserting a unique email address, or adding or deleting blank lines, etc.—the Fuzzy 1 and Fuzzy 2 hashes use different algorithms that take these minor differences into account, and create a hash based on that. If any one of the three thresholds is reached or exceeded, the specified action will occur.

SLS may be configured to contribute to the ESP Profile score, or to take action on its own in the SuperQueue. When SLS is to be processed in the Anti-Spam feature, Anti-Spam must be enabled, running, and assigned a "queue position."



The Statistical Lookup Service page invites the following user input:

Enable Statistical Lookup Service	Select the **Enable Statistical Lookup Service** check box to turn on SLS.
	Onsite SLS Settings
Current SLS Server	This field displays the name for the current SLS server.
Enable Onsite SLS	The checkbox enables or disables SLS functionality.
Onsite SLS Server IP	Enter the IP address for the onsite SLS server.
Onsite SLS Server Port	Enter the port number for the onsite SLS server.
SLS Client ID	Enter the authenticated client ID for the on-site SLS server.
SLS Client Password	Enter the password for the **SLS Client ID**.
Default SLS Server	Select the name of the default server from the pick list.
Enable Fallback to SLS-Ring	The checkbox enables or disables the fallback option.
Fallback SLS Server	Select the name of the fallback server from the pick list.
	SLS Settings
Hash Type	The **Hash Type** column reports three types of hashes: Body, Fuzzy 1, and Fuzzy 2. The Body hash represents the message body as it exactly is; the Fuzzy 1 and Fuzzy 2 hashes use different algorithms that take minor differences in a message body into account, and create hashes based on that.
Threshold	For each hash type, enter a numeric threshold. Do not enter a zero value. Entering a zero will cause SLS to determine that every message it receives is spam.
Action	IronMail can perform one of 8 actions if an SLS threshold is reached or exceeded. Select an action from the **Action** pick list. Note that some actions require qualifying information to be entered in the **Action Data** field immediately below. • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the **Action Data** input field below. For example, messages that reach or exceed an SLS threshold can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the **Action Data** input field immediately below. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the **Action Data** column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the

	ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Data** field indicating how many days the message remains in the queue before being returned to the normal mail flow, or that it should be deleted on IronMail's Cleanup Schedule. • **Log:** IronMail will deliver the message, but record in its Detailed SPAMQ Log that the message reached or exceeded the SLS threshold. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** Re-route is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action. When it is enabled, the user will see the re-route action as part of the spam *policy* definitions.
Action Data	Some actions require qualifying information. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not enter spaces between commas and subsequent email addresses.) • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. (Do not enter spaces between commas and subsequent email addresses.) • **Add Header:** A text string is required and must follow the RFC822 *protocol* rules for custom headers. The custom header format is: "**headername:headervalue**" where **headername** is an arbitrary name for the custom header, and **headervalue** is an arbitrary text string to display in the header. A sample custom header might be: "**HA-SPAM: 50**" ("**HA-SPAM**" is shorthand for "Header Analysis detected this message as SPAM," and "**50**" represents the policy's threshold. The header value string to the right of the colon cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** This action requires the *host name* and address of the IronMail appliance to which messages will be re-routed.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** pick list is enabled. A Queue must be specified.

Administrators may look in the Detailed SPAMQ Log to see the counts that the SLS server returned for each hash. (Note that the Anti-Spam Queue's Log Level must be set to "6"—*Queue Manager > Configure Queues > Queue-Anti-Spam*—to record this level of detail.) See Viewing Detailed Log Files for instructions on viewing message details in the SpamQ log.

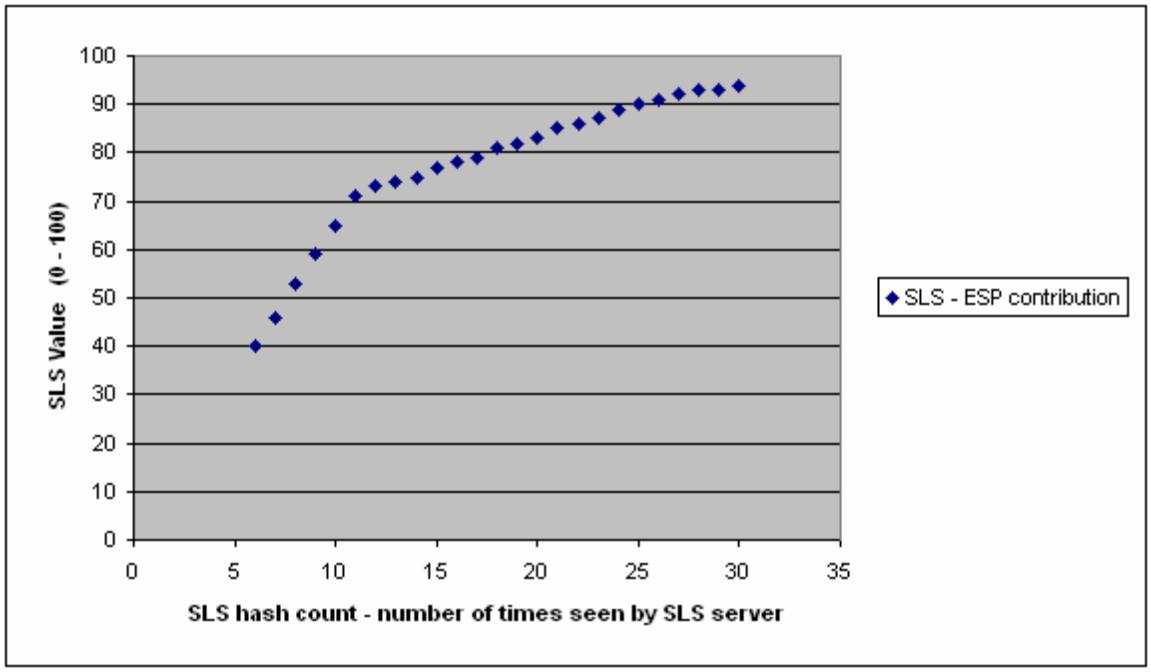
SLS Bypass

IronMail can be configured (Queue Manager > Configure Queues > Internal Queue *MIME* Ripper) to allow specific message types to bypass the Statistical Lookup Service check. This feature is primarily intended for read receipts and delivery receipts. If so enabled, the Rip Queue checks message headers for indications that the message is either a read receipt or a delivery receipt. If either of those conditions is true, the message bypasses the SLS check.

Currently, the SLS bypass functionality is only available for read receipts on Microsoft Outlook and Outlook Express, and delivery receipts on Microsoft Exchange servers.

SLS and ESP

Statistical Lookup Service returns two different values. To the SLS tool itself, it returns the actual number of times the particular message has been seen by the SLS server. However, the value returned to ESP is rated on a curve so the value will always be within the range of 0 to 100 points. The curve is shown below.



Value	SLS value based on where the number of messages seen intersects the predetermined curve. Confidence value: a pre-configured percentage.
Formula	ESP Contribution = SLS value X Confidence %
Example	ESP Contribution = 65 X 20% = 32 pts. where 65 is the curve value for 10 occurrences of the hash.

Analyzing Headers

Regular Expression Header Analysis

IronMail uses regular expressions in processing header analysis. Header fields can be matched against *regular expression* rules, or can be examined using functions. All the regular expressions are compiled at initialization to avoid the necessity to compile them in each thread of the SuperQueue.

Spam functionality reads the Ct_spam_service_list table at initialization. If the active spam service is a *regex* function, Spam Queue reads the regex_id field. If that field contains a value, the feature parses the value to extract regex identifiers (a comma-separated list of regex pattern identifiers). For each pattern found, IronMail calls a function to compile it and return a regex object. If the spam service that is processing the message is a regex function and a function name is present in the function_name field, this indicates the need for functional analysis. Each function may use none, one or more of the regex objects.

All regex definitions and function definitions are compiled in a separate file. IronMail is delivered with the current version of the file, and the file can be updated as part of CipherTrust's update system.

Note: The user cannot enter regular expressions independently, but may contact CipherTrust Support to request additions.

When the Spam Queue processes messages, it executes the regular expressions by passing the regex objects, data from the mail part of the message, and the method (search/replace) as arguments for the spam detection process. If the process finds a match, it records the configured point value. The functions also execute and the points are totalled. When total points exceed the configured threshold value, the spam service takes action based on the rules.

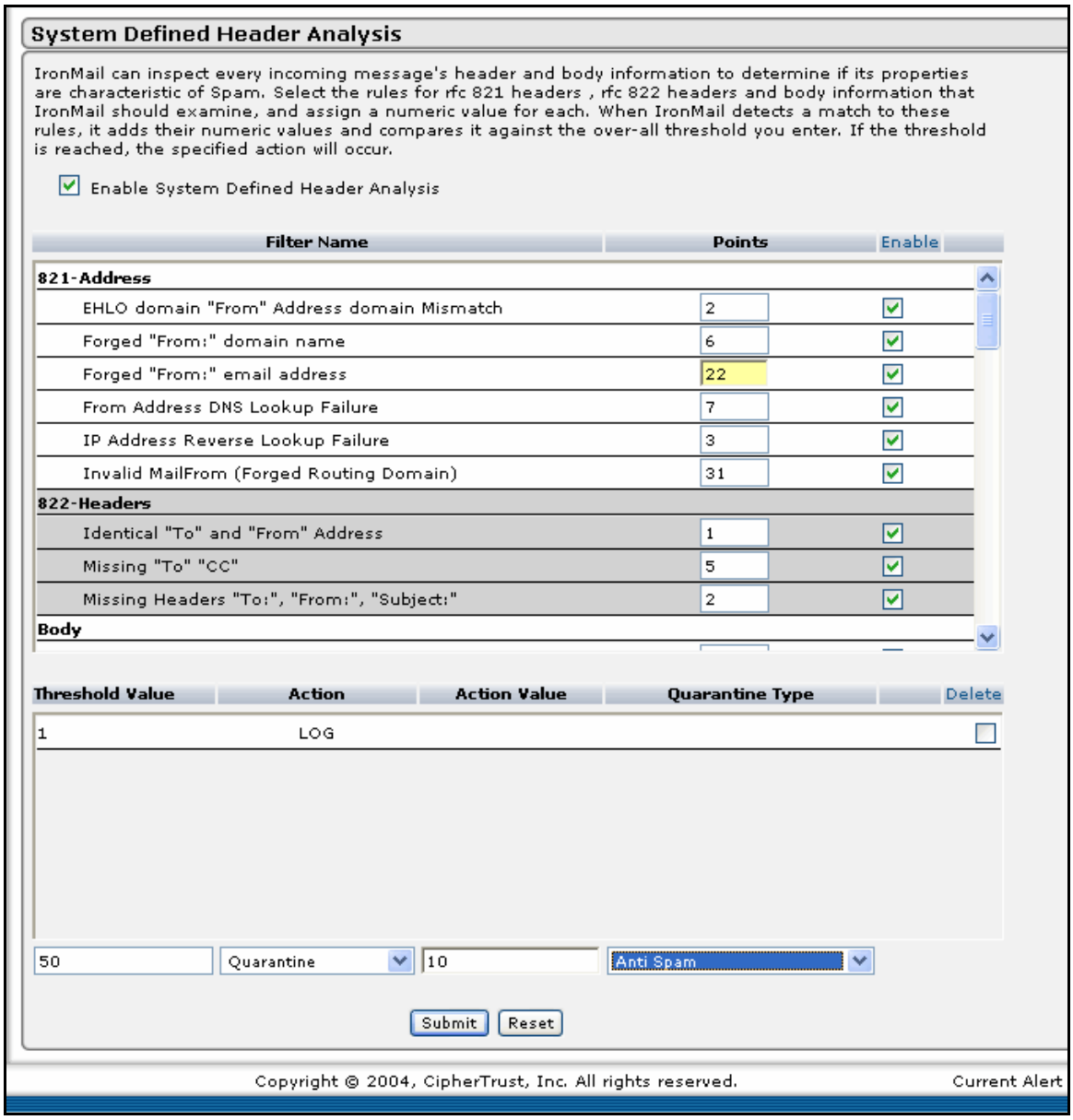
System Defined Header Analysis

IronMail's System Defined Header Analysis filters examine characteristics of the RFC822 headers.

System Defined Header Analysis is processed in the Anti-Spam feature. Therefore, Anti-Spam must be enabled and running for this tool to function.

Note that if a single message contains more than 175 total entries in the From, To, CC, or BCC headers, Anti-Spam will *not* process that message. The message remains in the SuperQueue until all applicable functionality has been applied to it.

Select the **Enable System Defined Header Analysis** check box to turn on System Defined Header Analysis.


System Defined Header Analysis
IronMail can inspect every incoming message's header and body information to determine if its properties are characteristic of Spam. Select the rules for rfc 821 headers , rfc 822 headers and body information that IronMail should examine, and assign a numeric value for each. When IronMail detects a match to these rules, it adds their numeric values and compares it against the over-all threshold you enter. If the threshold is reached, the specified action will occur.
Enable System Defined Header Analysis
Filter Name
Points
Enable
821-Address
EHLO domain "From" Address domain Mismatch
2
Forged "From:" domain name
6
Forged "From:" email address
22
From Address DNS Lookup Failure
7
IP Address Reverse Lookup Failure
3
Invalid MailFrom (Forged Routing Domain)
31
822-Headers
Identical "To" and "From" Address
1
Missing "To" "CC"
5
Missing Headers "To:", "From:", "Subject:"
2
Body
Threshold Value
Action
Action Value
Quarantine Type
Delete
1
LOG
50
Quarantine
10
Anti Spam
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert

The System Defined Header Analysis page is broken into two parts: a list of "filters" that look for specific header information, and a table of policies specifying what actions IronMail should take when certain thresholds are reached.

Field	Description
Filter Name	This column is segmented by the message part to which it applies. For each part, the applicable SDHA rules are listed. The list of rules is discussed separated.
Points	Beside each filter, this column shows the point score assigned to each filter. These scores are editable.
Enable	Clicking the Enable checkbox beside a filter enables that specific filter. Clicking the Enable hyperlink enables all filters.

Table of Policies	***The lower portion of the screen displays all configured policies for SDHA. The user may also add or delete policies.***
Threshold Value	This columns shows the threshold that logically relates to the individual "point values" for the enabled filters above. If a message triggers any enabled filters, their point values are summed, and if the total meets or exceeds this threshold, the specified action is taken.
Action	This column shows the action specified for the associated *policy*. Options are: • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value field. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must appear in the Action Value field. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the Action Value field. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the Quarantine Type column will list the quarantine chosen. • **Log:** IronMail will deliver the message, but record in its Detailed SPAMQ Log that the message reached or exceeded a header analysis threshold. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** This is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the spam policy definitions.
Action Value	Some actions require qualifying information. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Add Header:** A text string is required and must follow the RFC822 *protocol* rules for custom headers. The custom header format is: "headername:headervalue" where headername is an arbitrary name for the custom header, and headervalue is an arbitrary text string to display in the header. A

	sample custom header might be: "HA-SPAM: 50" ("HA-SPAM" is shorthand for "Header Analysis detected this message as SPAM," and "50" represents the policy's threshold. The header value string to the right of the colon cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** this option requires a *host name* and address for the dedicated IronMail appliance to which messages are to be re-routed.
Quarantine Type	When the Quarantine action is selected, the Quarantine Type will be specified.
Delete	Select a policy's **Delete** check box and click **Submit** to delete the policy from this table.

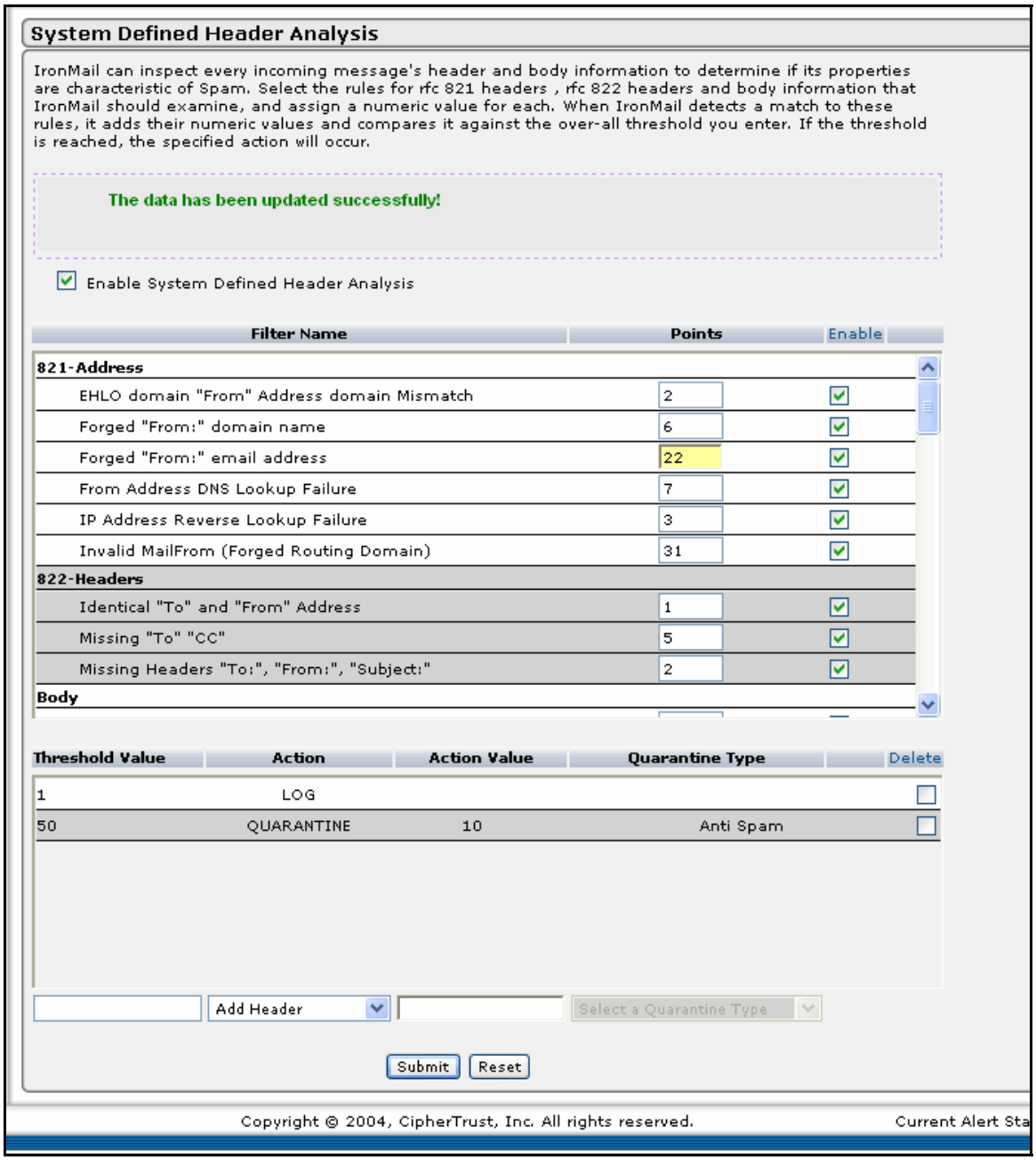
Adding a New Policy

The Administrator can add new policies by entering the necessary data in the fields just below the Table of Policies on the SDHA screen. The fields correspond to the columns in the Table of Policies.

Field	Description
Threshold Value	Enter a number, from 1 to 99,999, that logically relates to the individual "point values" for the enabled filters above. This number represents the action threshold for the specific policy. If a message has characteristics detected by any of the enabled filters, their point values are summed, and if the total meets or exceeds this threshold, the specified action is taken.
Action	IronMail can perform one of several actions if a threshold is reached or exceeded. Select an action from the Action pick list. Note that some actions require qualifying information to be entered in the Action Value field immediately below. • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value input field below. For example, messages that reach or exceed a header analysis threshold can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the Action Data input field immediately below. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that

	contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Data** field indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Log:** IronMail will deliver the message, but record in its Detailed SPAMQ Log that the message reached or exceeded a header analysis threshold. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** This is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the spam policy definitions.
Action Value	Some actions require qualifying information. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Add Header:** A text string is required and must follow the RFC822 protocol rules for custom headers. The custom header format is: "headername:headervalue" where headername is an arbitrary name for the custom header, and headervalue is an arbitrary text string to display in the header. A sample custom header might be: "HA-SPAM: 50" ("HA-SPAM" is shorthand for "Header Analysis detected this message as SPAM," and "50" represents the policy's threshold. The header value string to the right of the colon cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** this option requires a host name and address for the dedicated IronMail appliance to which messages are to be re-routed.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** pick list is enabled. A Queue must be specified.

When all the data is complete, click **Submit**. The Table of Policies will be updated.


System Defined Header Analysis
IronMail can inspect every incoming message's header and body information to determine if its properties are characteristic of Spam. Select the rules for rfc 821 headers , rfc 822 headers and body information that IronMail should examine, and assign a numeric value for each. When IronMail detects a match to these rules, it adds their numeric values and compares it against the over-all threshold you enter. If the threshold is reached, the specified action will occur.
The data has been updated successfully!
Enable System Defined Header Analysis
Filter Name
Points
Enable
821-Address
EHLO domain "From" Address domain Mismatch 2
Forged "From:" domain name 6
Forged "From:" email address 22
From Address DNS Lookup Failure 7
IP Address Reverse Lookup Failure 3
Invalid MailFrom (Forged Routing Domain) 31
822-Headers
Identical "To" and "From" Address 1
Missing "To" "CC" 5
Missing Headers "To:", "From:", "Subject:" 2
Body
Threshold Value
Action
Action Value
Quarantine Type
Delete
1 LOG
50 QUARANTINE 10 Anti Spam
Add Header
Select a Quarantine Type
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Sta

Header Analysis Filters

IronMail will use any of the filters enabled on this page as it examines each message entering the Anti-Spam Queue. Each enabled filter must be given an associated numeric "weight" or "point" value. The point values are arbitrary, but they must relate logically to the over-all threshold specified for each System Defined Header Analysis *policy*. (Administrators may use the point value as a "binary" value—e.g., on or off—where all filters have the same point value and the over-all threshold simply becomes a count of how many filters detected certain header characteristics. Alternately, administrators may use varying point values to reflect their confidence that a particular header characteristic is correctly associated with spam. The over-all threshold becomes, then, a weighted scale, where a target has to be reached before IronMail will act on the message.)

Group	*Rule*	Help Text
821-Address	Forged "From:" email address	IronMail will check that the RFC822 FROM email address is in the proper format and compare this address with the FROM email address in the RFC821 header.
821-Address	Forged "From:" domain name	IronMail will check that the RFC822 FROM *domain name* is in the proper format (domain + dot + com/net/org, etc.) and compare this address with the FROM domain name in the RFC821 header.
821-Address	From Address DNS Lookup Failure	IronMail will do an MX lookup for the RFC822 From address domain.
821-Address	EHLO domain "From" Address domain Mismatch	IronMail compares the EHLO domain name it receives in the initial SMTP handshake with the From address domain name.
821-Address	*IP Address* Reverse Lookup Failure	IronMail will do a reverse lookup for the IP address from which a connection came and compare it with the result of the MX lookup of the EHLO domain. Note: Because IronMail gets the result of the MX lookup of the EHLO domain, this option does not require that the previous option, EHLO domain From address domain mismatch option, be enabled.
821-Address	Invalid MailFrom (Forged Routing Domain)	Ironmail will detect addresses that are a part of the routing domain and not in the allow relay IP list.
822-Headers	Missing Headers "To:", "From:", "Subject"	IronMail will detect any message that does not contain a RFC822 To or From address, or Subject line. (Be aware that end users frequently send email that does not contain a Subject line.)
822-Headers	Identical "To" and "From" Address	IronMail will detect if an identical email address is present in both the To and From addresses.

822-Headers	Missing "To" "CC"	IronMail will require that at least one value is present in either the To or Copy headers. Only if a value is not present in either header does this filter “flag” a message.
CC-Address	Multiple headers	IronMail will detect messages with more than 150 addresses present in the CC headers.
Date	Timezone does not exist	IronMail will not allow TimeZone > + 1400 and < -1400
Date	More than 96 hrs old or 24 to 96 hrs before time	IronMail will detect if the date header value is 96 hrs in past or 24-96 hrs in future of received header dates
Date	Does not conform to rfc 822	IronMail detects if the rfc 822 date header value does not follow the rfc 822 specifications
Date	Unusual Y2K formatting	IronMail detects if the date header does not follow normal Y2K date formatting.
From-Address	Contains "at something-offers"	IronMail detects if the rfc 822 from address contains the word ‘offers’ in the domain name e.g. abc@cooloffers.com
From-Address	Contains No Local part before @ sign	IronMail will detect addresses that start with @ which will catch faulty mail ids like abc @ abc.com<abc@abc.com>
From-Address	Contains 3 consecutive 8 bit characters	IronMail detect if there are 3 consecutive 8 bit characters in from address. \x80-\xff are 8 bit characters
From-Address	Mixed with numbers starting with a letter	IronMail checks for From addresses that have numbers mixed with letters, but starting with a letter.
From-Address	Contains numbers	IronMail checks for From addresses that have numbers mixed with letters in a special pattern

From-Address	Ends with numbers	IronMail checks for From addresses that end with numbers
Message-Id	Forged Message ID	Email servers automatically generate a unique message ID when sending a message. IronMail first checks that there is a message ID, then checks that it is properly enclosed within open and closed angle brackets (“<” and “>”), and that it contains a domain name.
Message-Id	Pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of alphanumeric characters generated very often by spam tools
Message-Id	Zeroes Variant Pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of zeroes generated very often by spam tools
Message-Id	6-letter Variant pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of alphanumeric characters generated very often by spam tools
Message-Id	3-Dollars variant pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of dollars and digits generated very often by spam tools
Message-Id	4 Zeroes variant pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of four zeroes generated very often by spam tools
Message-Id	4 Numbers and Dollars variant pattern indicates generation by spam tool	Ironmail detects invalid Message Id format containing a defined pattern of dollars and four digits generated very often by spam tools
Message-Id	Contains no hostname	Ironmail detects invalid Message Id format with no information of hostname following @ symbol

MS Outlook Specific	Missing Outlook name	IronMail checks to see if the message has been forged to have been sent from Microsoft Outlook
Received	Contains indication of receipt via buggy SMTP server (MDaemon 2.7.4SP4R)	Ironmail detects if one of the received header contains ‘with SMTP .MDaemon.v2.7.SP4.R.’
Received	Contains a spam-sign i.e. lowercase smtp	Ironmail detects if one of the received header contains ‘with smtp;’
Received	Contains 'CacheFlowServer' IDENT name	Ironmail detects if the received headers indicate that the message was sent by a squid proxy.
Reply-To-Address	Is Empty	Ironmail detects that the header is present but contains nothing.
Subject	Starts with To address	IronMail detects that the subject line begins with the To address
Subject	Not present and empty body	IronMail detects that there is no subject, and that the body of the message is empty
Subject	Present and empty body	IronMail detects that the subject is present, but the body of the message is empty
Subject	Contains both exclamation and question mark	Ironmail detects a subject which contains exclamation as well as question mark in any order meaning that any one can precede the other and be separated by words or white space.
Subject	Starts with advertising tag	Ironmail detects that the subject starts with the letters ADV.
Subject	Contains advertising tag	Ironmail detects that the subject contains the letters ADV which may be interspersed with white spaces.
Subject	Contains 'As Seen'	Ironmail detects subject header containing word ‘As seen’
Subject	Contains " Free Instant"	Ironmail detects subject header containing word ‘Free Instant’
Subject	Starts with 'Free'	Ironmail detects subject header that starts with the word ‘Free’

Subject	Contains GUARANTEED	Ironmail detects subject header containing word ‘Guaranteed’
Subject	Contains 'life insurance'	Ironmail detects subject header containing word ‘life insurance’
Subject	Contains 'Now Only'	Ironmail detects subject header containing words ‘now only’
Subject	Contains 'viagra'	Ironmail detects subject header containing word ‘viagra’
Subject	Contains 'Your Family'	Ironmail detects subject header containing words ‘your family’
Subject	Contains statement on losing pounds	Ironmail detects subject header which contains statements like lose pounds /lose weight/ lose lbs or similar
Subject	Contains statement about being approved	Ironmail detects subject header which contains words like approved or approval
Subject	Indicative of Nigerian spam	Ironmail detects subject header which contains statements like Re: very urgent and confidential
Subject	Contains Nigerian spam words	Ironmail detects subject header which contains statements like Re: family assistance
Subject	Contains Korean unsolicited email tag	Ironmail detects subject header which contains 8 bit characters where "/xbc/xba/xc0/xce means 'adult' /xb1/xa4/xb0/xed means 'advertisement' \xc1\xa4\xba\xb8 means 'information' \xc8\xab\xba\xb8 means 'publicity’ indicative of a Korean spam.
Subject	Contains lot of 8 bit characters	Ironmail detects subject header which contains 8 bit characters \x80-\xff are 8 bit characters
To-Address	Contains 3 consecutive 8 bit characters	Ironmail detects if there are 3 consecutive 8 bit characters in To address. \x80-\xff are 8 bit characters

Note that a missing or forged domain name—something frequently encountered in e-newsletters—will potentially be detected by the *Forged From Email Address*, *Forged From Domain Name*, and *EHLO Domain From Address* filters. Administrators may wish to set a lower weight for these filters so that this one piece of "bad information" does not automatically trigger a low threshold.

Administrators may look in the Detailed SPAMQ Log to see which message header characteristics indicated that the message was a spam. (Note that the Anti-Spam Queue's Log Level must be set to "6"—*Queue Manager > Configure Queues > Queue-Anti-Spam*—to record this level of detail.) See Understanding Detailed Logs for information on viewing message details in the SpamQ log.

RFC821 versus RFC822 Headers

The RFC821 (Request for Comment 821) and RFC822 documents (also known as Internet Official *Protocol* Standards 10 and 11) are documents that describe the specifications for technologies used for Internet messaging.

Every email contains two sets of "headers" that identify the message sender, recipient, data, subject, etc.:

- **RFC821 Headers:** These are the headers that have to do with delivery of the mail over the internet and are the "envelope headers" and are described in RFC821. This is the data exchanged between sending and receiving servers as they negotiate how the message is to be delivered.

  Since it is less frequently counterfeited, RFC821 information is more reliable than RFC822 data for use in capturing true spam while allowing legitimate email to be delivered. IronMail displays RFC821 header data everywhere in the Queue Manager program area except in the Message Details window. IronMail's whitelists and blacklists are based on the RFC821 header data.

- **RFC822 Headers:** These are "content headers" that describe the content of the message. Content headers can also contain information that is particular to specific mail delivery systems. This is the data the email program uses when displaying the email in its interface. The User Spam Reporting table displays the RFC822 header data.

SDHA and ESP

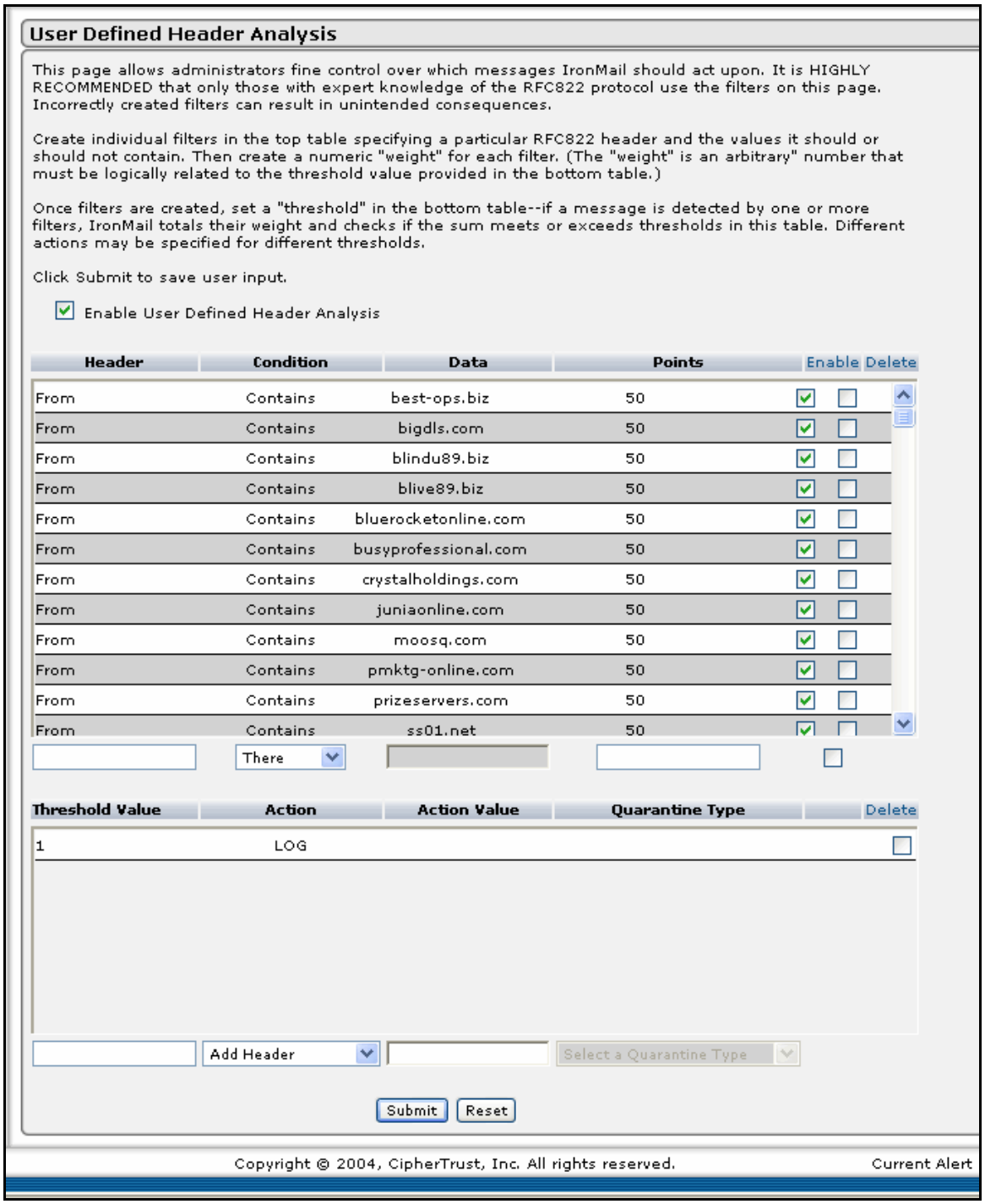
System-Defined Header Analysis returns an absolute point value to ESP. Each SDHA filter that is configured in the SDHA screen has an associated point value. Each of these values (all positive numbers) is returned to ESP.

Values	The configured point value for each triggered SDHA filter.
Formula	ESP Contribution = Sum of all matched SDHA filter points.
Example	Invalid MailFrom (Forged Routing Domain): 10 points Date does not conform to RFC822: 15 points ESP Contribution = 10 + 15 = 25 points.

User Defined Header Analysis

This page allows administrators fine control over which messages IronMail should act upon. It is highly recommended that only those with expert knowledge of the RFC822 *protocol* create and use the filters on this page. Incorrectly created filters can result in unintended consequences.

Create individual filters in the top table specifying a particular RFC822 header and the values it should or should not contain. Then create a numeric "weight" for each filter. (The "weight" is an arbitrary number that must be logically related to the threshold value provided in the bottom table.) Depending on the over-all threshold, when some combination of filters identifies spam-like header characteristics in a message, IronMail will take an action.


User Defined Header Analysis
This page allows administrators fine control over which messages IronMail should act upon. It is HIGHLY RECOMMENDED that only those with expert knowledge of the RFC822 protocol use the filters on this page. Incorrectly created filters can result in unintended consequences.
Create individual filters in the top table specifying a particular RFC822 header and the values it should or should not contain. Then create a numeric "weight" for each filter. (The "weight" is an arbitrary" number that must be logically related to the threshold value provided in the bottom table.)
Once filters are created, set a "threshold" in the bottom table--if a message is detected by one or more filters, IronMail totals their weight and checks if the sum meets or exceeds thresholds in this table. Different actions may be specified for different thresholds.
Click Submit to save user input.
Enable User Defined Header Analysis
Header
Condition
Data
Points
Enable
Delete
From Contains best-ops.biz 50
From Contains bigdls.com 50
From Contains blindu89.biz 50
From Contains blive89.biz 50
From Contains bluerocketonline.com 50
From Contains busyprofessional.com 50
From Contains crystalholdings.com 50
From Contains juniaonline.com 50
From Contains moosq.com 50
From Contains pmktg-online.com 50
From Contains prizeservers.com 50
From Contains ss01.net 50
There
Threshold Value
Action
Action Value
Quarantine Type
Delete
1 LOG
Add Header
Select a Quarantine Type
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert

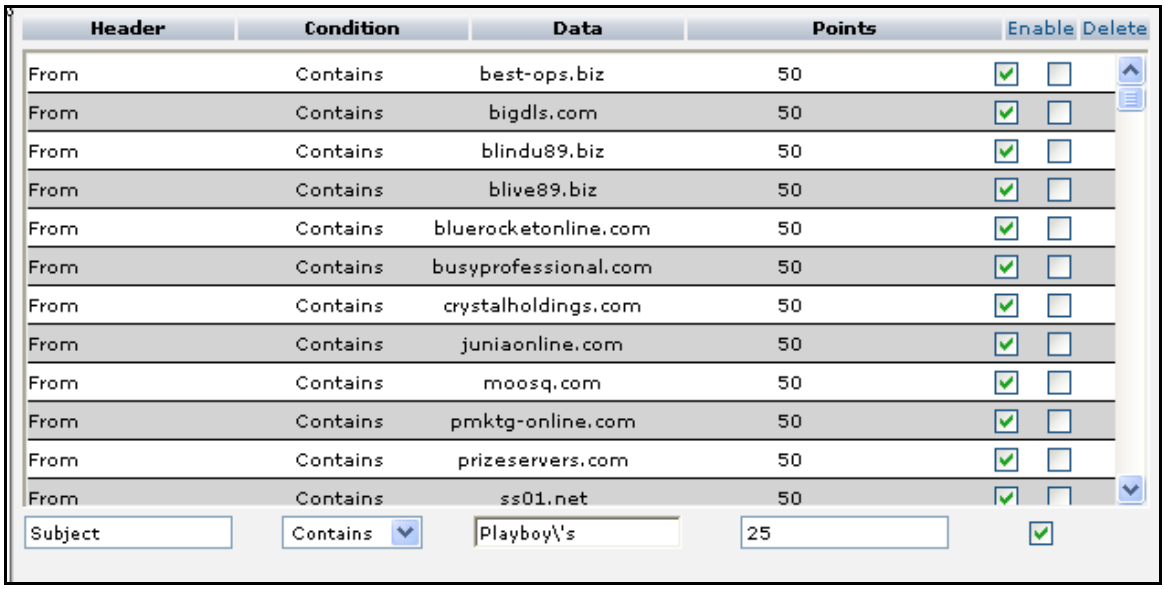
Select the **Enable User Defined Header Analysis** check box to turn on User Defined Header Analysis.

The table of filters remains empty until filters have been created. Each of the filters has been defined based upon "user" input. Instructions for creating new filters will be explained below.

Field	Description
Header	This column displays the name of the RFC822 header type upon which the filter is based. An X in front of the name indicates that it is a custom header type created by a User (e.g., X-Mime-Key).
Condition	This column displays one of four values: • **There:** the specified header is present. • **Not There:** the specified header is not present. • **Equal To:** the specified header exactly matches the text string appearing in the Data column to the right. • **Contains:** the text string appearing in the Data column to the right appears anywhere in the specified header.
Data	This column displays the text string that the User Defined Header Analysis *policy* is expecting to be present or not present in the specified header. **Note:** An entry in the column is required for the **Equal To** and **Contains** conditions.
Points	This column displays the "point" value or "weight" of a given filter. The number is arbitrary, but relates logically to the over-all thresholds indicated in the User Defined Header Analysis policy table below.
Enable	Clicking the check box for a specific filter enables or disables that filter. Clicking the Enable hyperlink enables or disables all filters.
Delete	Select a filter's Delete check box and click **Submit** to delete a filter from this table.
Table of Policies	***The lower portion of the screen displays all configured policies for UDHA. The user may also add or delete policies.***
Threshold Value	This column displays the threshold for the associated policy.
Action	The column shows the action configured for the specific policy.
Action Value	If an action value is required for the selected action, it will display in this column.
Quarantine Type	If the selected action is Quarantine, the Quarantine Type is listed in this field.
Delete	Select any policy's Delete check box and click **Submit** to delete that policy from this table. Click the Delete hyperlink to delete all policies.

Adding Rules and Policies

The User Defined Header Analysis screen provides input fields for adding new filters to the list. The data fields just below the Table of Filters must be completed.



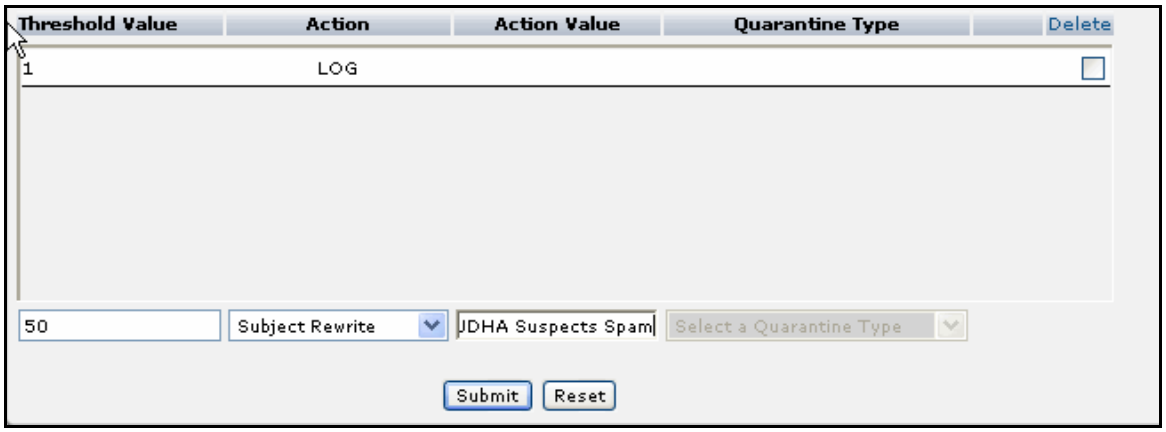
Header	Condition	Data	Points	Enable	Delete
From	Contains	best-ops.biz	50	☑	☐
From	Contains	bigdls.com	50	☑	☐
From	Contains	blindu89.biz	50	☑	☐
From	Contains	blive89.biz	50	☑	☐
From	Contains	bluerocketonline.com	50	☑	☐
From	Contains	busyprofessional.com	50	☑	☐
From	Contains	crystalholdings.com	50	☑	☐
From	Contains	juniaonline.com	50	☑	☐
From	Contains	moosq.com	50	☑	☐
From	Contains	pmktg-online.com	50	☑	☐
From	Contains	prizeservers.com	50	☑	☐
From	Contains	ss01.net	50	☑	☐
Subject	Contains	Playboy\'s	25	☑	

Below the table of filters are four user-input fields. These fields, matching the columns in the table, allow the user to define new filters for UDHA.

Field	Description
Header	Enter the name of a valid or custom RFC822 header-type upon which to base the new filter.
Condition	Select one of the four options specifying the filter's condition: • **There:** the value in the Data field is characteristic of spam—when it is there, the filter will "flag" the message as possible spam. • **Not There:** the value in the Data field is expected in normal email—when it is not there, the filter will "flag" the message as possible spam. • **Equal To:** the value in the Data field is characteristic of spam—if the header contains the exact string, the filter will flag the message as possible spam. • **Contains:** the value in the Data field is characteristic of spam—when the header contains the string anywhere within the header, the filter will flag the message as possible spam.
Data	Enter a text string that is characteristic of spam or characteristic of normal email. Depending on the condition specified in the "Condition" field above, IronMail will check if this string is present in or absent from the header and make a determination whether or not the message is likely to be spam. If you want to add a data value that includes an apostrophe, you must escape that apostrophe, as shown below: Subject contains Mike\'s.
Points	Enter a number representing how confidently the filter may be trusted to detect spam without generating false positives. The number is arbitrary, but must relate logically to the over-all threshold created in a User Defined Header Analysis policy below.
Enable	If you want the policy to be enabled immediately, click the Enable check box.

Click **Submit** to save the user input.

Once filters have been created, build User Defined Header Analysis policies in the bottom table—if one or more filters detect specified header characteristics, IronMail totals the filters' weight and checks if their sum meets or exceeds thresholds in this table. Different actions may be specified for different thresholds.



Beneath the table of User Defined Header Analysis policies are four input fields inviting the following user input:

Field	Description
Threshold Value	Enter a number, from 1 to 99,999, that logically relates to the individual "point values" for the enabled filters above. If a message has RFC822 characteristics detected by any of the enabled filters, their point values are summed, and if the total meets or exceeds this threshold, the specified action is taken.
Action	IronMail can perform one of actions if a threshold is reached or exceeded. Select an action from the Action pick list. Note that some actions require qualifying information to be entered in the Action Value field immediately below. • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value input field below. For example, messages that reach or exceed a header analysis threshold can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the Action Data input field immediately below. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field to the right. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must

	be entered in the **Action Data** field indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Log:** IronMail will deliver the message, but record in its Detailed SPAMQ Log that the message reached or exceeded a header analysis threshold. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** This is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the spam policy definitions.
Action Value	Some actions require qualifying information. • **Subject rewrite:** A text string is required. A maximum of 254 characters are allowed, and may be any printable character on the keyboard. • **Copy Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Forward Message:** A valid email address is required. Multiple email addresses must be separated from each other with commas. • **Add Header:** A text string is required and must follow the RFC822 protocol rules for custom headers. The custom header format is: "headername:headervalue" where headername is an arbitrary name for the custom header, and headervalue is an arbitrary text string to display in the header. A sample custom header might be: "HA-SPAM: 50" ("HA-SPAM" is shorthand for "Header Analysis detected this message as SPAM," and "50" represents the policy's threshold. The header value string to the right of the colon cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.) • **Quarantine:** A number is required indicating how many days the message remains in the queue before being returned to the normal mail flow. • **Re-route:** This action requires a *host name* and address for the dedicated IronMail appliance to which messages will be re-routed.
Quarantine Type	When the Quarantine action is selected, the **Quarantine Type** pick list is enabled. A Queue must be specified.
Delete	Select a policy's **Delete** check box and click **Submit** to delete the policy from this table.

Click **Submit** to save user input.

UDHA and ESP

User-Defined Header Analysis returns an absolute point value to ESP. Each UDHA filter that is configured in the UDHA screen has an associated point value. Each of these values (all positive numbers) is returned to ESP.

Values	The configured point value for each triggered UDHA filter.
Formula	ESP Contribution = Sum of all matched UDHA filter points.
Example	X-List-Unsubscribe: 10 points X-Library : 5 points ESP Contribution = 10 + 5 = 15 points.

Sender Policy Framework

Sender Policy Framework

Sender *Policy* Framework (SPF) is an anti-spoofing tool that compares the envelope sender domain or HELO/EHLO domain against the client *IP address* before any message data is transmitted. The goal is to detect email address forgery - those messages wherein hackers and spammers have forged the "From" address, using either a totally fictitious IP or one they have stolen from a legitimate sender. The tool depends upon having domain owners designate sending email exchangers in DNS, to allow SMTP servers to distinguish legitimate email from illegitimate mail. While SPF is primarily an anti-forgery weapon, the user may also benefit from reduced spam and decreased vulnerability to viruses, worms, etc.

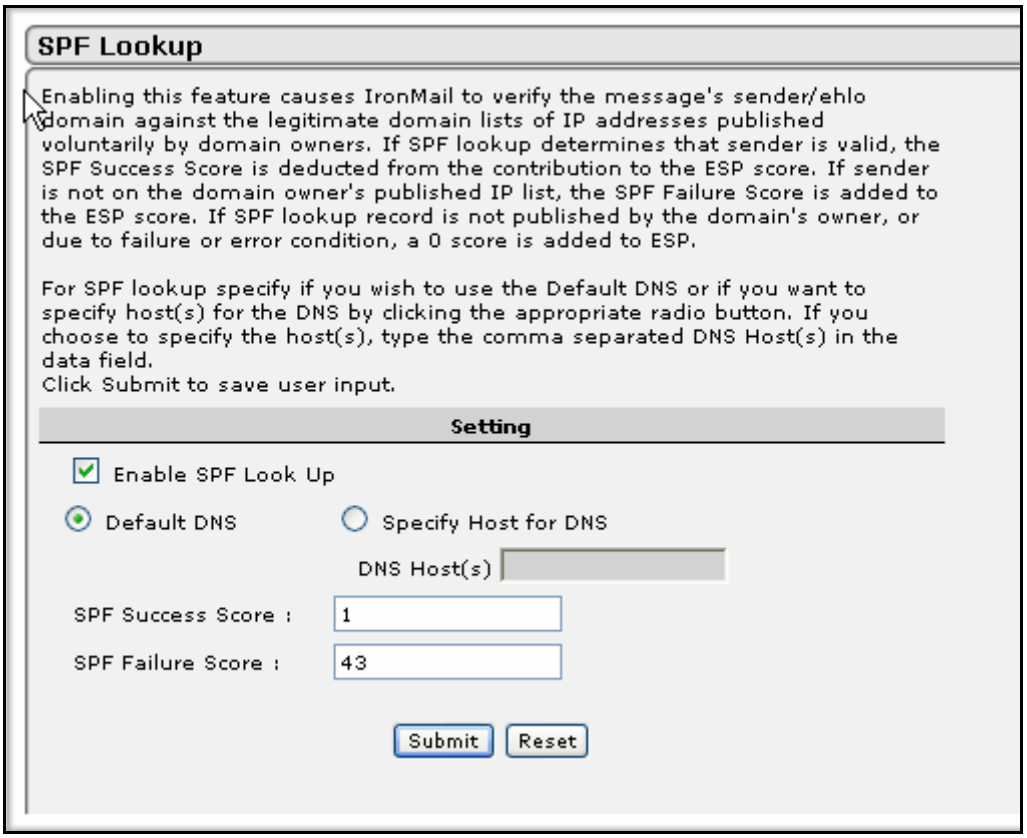
SPF does not verify individual sender usernames, but only validates the *domain name*. It does not protect the header "From:" address, only the envelope sender address. Each domain is responsible for publishing and maintaining its own SPF records.

SPF is extended SMTP, to prevent spammers from forging email domains. It is a counterpart of the MX list. SPF does not force he users to declare a domain for the MTA implementation (SPF client). It improves the veracity of the sender address.

IronMail's Implementation of SPF

While the Sender Policy Framework Lookup usually occurs before a message enters the *network*, IronMail implements SPF like a Reverse DNS Lookup, supporting only TXT queries. IronMail is simply an SPF client. SPF, if it is enabled, is configured to contribute to the ESP score. You may configure SPF using the window shown below (Anti-Spam > SPF Lookup).

You must also enable SPF on the ESP Configuration (Anti-Spam > Enterprise Spam Profiler > Configure) screen to allow the contribution to be accepted.


SPF Lookup
Enabling this feature causes IronMail to verify the message's sender/ehlo domain against the legitimate domain lists of IP addresses published voluntarily by domain owners. If SPF lookup determines that sender is valid, the SPF Success Score is deducted from the contribution to the ESP score. If sender is not on the domain owner's published IP list, the SPF Failure Score is added to the ESP score. If SPF lookup record is not published by the domain's owner, or due to failure or error condition, a 0 score is added to ESP.
For SPF lookup specify if you wish to use the Default DNS or if you want to specify host(s) for the DNS by clicking the appropriate radio button. If you choose to specify the host(s), type the comma separated DNS Host(s) in the data field.
Click Submit to save user input.
Setting
Enable SPF Look Up
Default DNS
Specify Host for DNS
DNS Host(s)
SPF Success Score :
1
SPF Failure Score :
43
Submit
Reset

Enabling SPF Lookup allows IronMail to verify the sender domain names against the "legitimate domain" lists of IP addresses published voluntarily by domain owners. From its lookup process, SPF determines one of the following responses:

- The sender is good (valid), meaning the IP address is listed in the owner's published IP list); SPF Lookup sends the SPF Success Score to be deducted from the total ESP score.
- The sender is bad (not on the domain owner's published IP list); SPF Lookup sends the SPF Failure Score to be added to the ESP profile score.
- SPF encounters an error (syntax, etc.) or doesn't recognize the domain because the domain owner has not published IP addresses; SPF sends a contribution of zero (0) points to ESP.

The following information is required on the SPF Lookup screen:

Field or function	Description
Enable SPF Look Up	Selecting this checkbox will enable the SPF functionality. **Note:** You must also enable SPF in the Enterprise Spam Profiler.
Select a Domain Name Service host	Click the Default DNS radio button to select the default host with its associated IP address Click the Specify Host for DNS radio button to specifyt an IP address or addresses other than the default. • If you click this radio button, you must also enter a host IP address or addresses in the DNS Host(s) data field.

Set an SPF Success score	Enter a number from 0 to 100 points to be *deducted* from the ESP profile score when SPF determines that a message should be permitted into the network (the message passes). The default is 10 points.
Set an SPF Failure score	Enter a number from 0 to 100 points to be contributed to the ESP profile total score when SPF determines that a message should not be permitted (the message fails)..

When you have entered the necessary information, click Submit to execute your choices. If you decide to return the screen to its original state without saving your changes, click Reset.

SPF and ESP

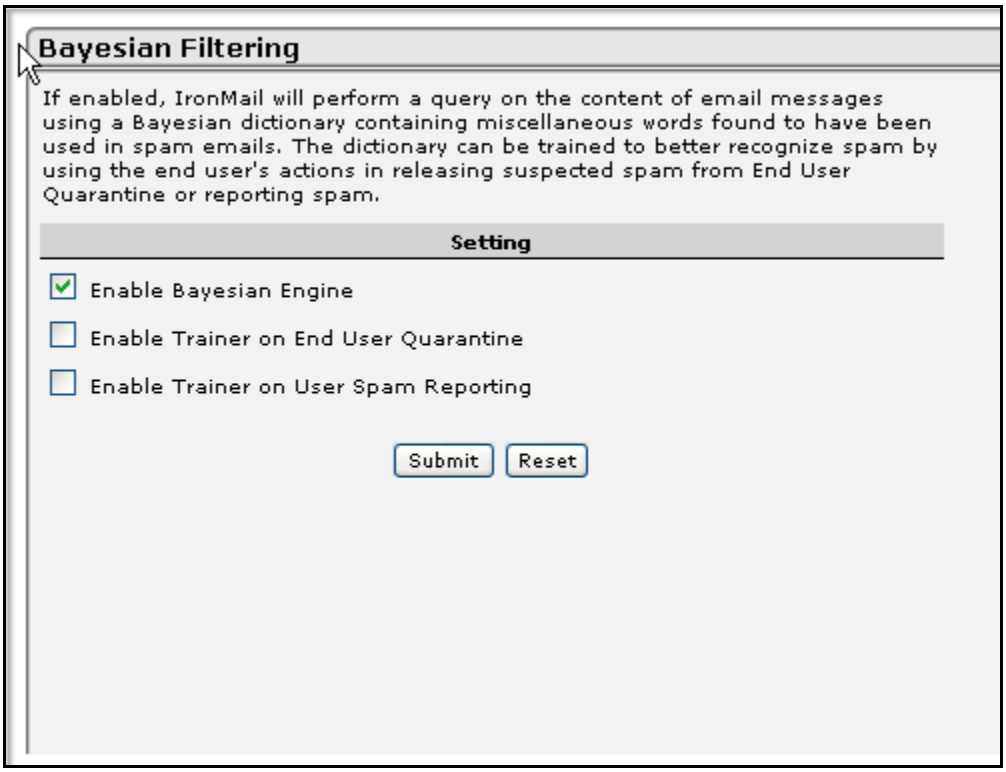
The Sender *Policy* Framework lookup results in an absolute value that is contributed to ESP. If the lookup is ***successful*** (SPF+), the absolute value in the SPF Success Score will be returned as a ***negative*** contribution to ESP. If the SPF lookup is ***unsuccessful*** (SPF-), the value in the SPF Failure Score will be returned to ESP as a ***positive*** contribution.

Values	SPF lookup values (points)
Formula	ESP Contribution = SPF lookup value points.
Example	If the SPF lookup completed with a matching IP (SPF+) and the success score is 10 points, then: ESP Contribution = -10 points. If the SPF lookup completed without a matching IP (SPF-) and the failure score is 49 points, then: ESP Contribution = 49 points.

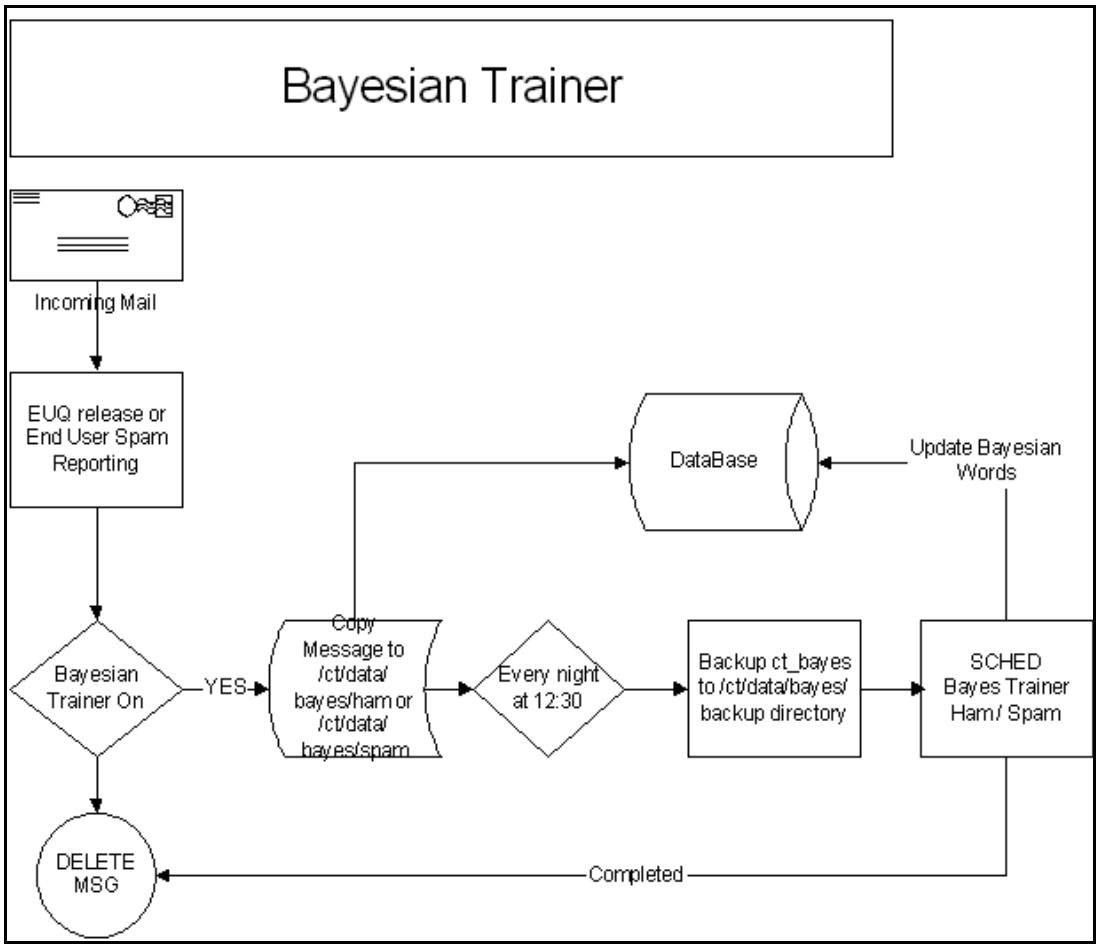
Bayesian Filtering

Bayesian Engine

The Bayesian Engine classifies incoming email messages as "ham" (good email), "spam" or "unsure" using probability theory. Spam or unsure messages can be diverted to a separate queue, etc., so as not to interrupt mail flow. The classification is based on clues from prior messages that the user has considered "spam" or "ham." The functionality is derived from the Python-based SpamBayes project.


Bayesian Filtering
If enabled, IronMail will perform a query on the content of email messages using a Bayesian dictionary containing miscellaneous words found to have been used in spam emails. The dictionary can be trained to better recognize spam by using the end user's actions in releasing suspected spam from End User Quarantine or reporting spam.
Setting
Enable Bayesian Engine
Enable Trainer on End User Quarantine
Enable Trainer on User Spam Reporting
Submit
Reset

IronMail includes a Bayesian word list, but it may also be "trained" by each user to identify the categories of email messages. This is done by showing it a large sample of emails the user considers legitimate and a sample of emails he considers spam. Bayesian Filtering analyses these samples for clues that differentiate them, such as different words, differences in mail headers, content style, etc. The clues are stored as a Bayesian Dictionary. The system then uses these clues to examine new messages. The Bayesian Engine contributes to the ESP profile based on the probability scores that result.



The Bayesian Engine can continually be trained based on messages included in User Spam Reporting and/or messages released under End User Quarantine Release. The continued training can be enabled on the Bayesian Filtering screen. If training is enabled, the training functions run every night at 12:30 to train the ct_bayes table with new words for ham and spam. Once the training is completed, each message is removed from the disk. Training exceptions generate a log entry, "Could not train the database for this message <file name>," then proceeds to the "delete" operation.

The Bayesian Engine contributes to the ESP score, and takes no action of its own. The scores are based on individual words used to calculate the probability that a message is spam. The probability score is used to calculate the yield to ESP using the confidence factor.

Bayesian Training Scenarios

Bayesian Training can be enabled on the Bayesian Filtering Screen, allowing the functionality to learn based on the customer's environment and maintain or increase its effectiveness. CipherTrust recommends that you set up training for both "spam" and "ham" as described below, if you plan to use this IronMail feature.

Each possible configuration has impact on effective filtering. Assuming that Bayesian filtering is enabled, you can set the function to train from Spam Reporting (both End User Spam Reporting and Enterprise Spam Reporting), End User Quarantine Release, both, or neither. The table below briefly describes the impacts of these options.

IF ...	THEN ...	Impact

Neither option is enabled,	The Bayesian Engine will not train at all.	The Bayesian word list will not change, and the effectiveness will remain as it is or perhaps decrease.
"Enable Trainer on End User Quarantine" is enabled,	The Bayesian Engine will learn about messages the end user considers "ham."	Bayesian Engine performance will improve pertaining to false positives.
"Enable Trainer on User Spam Reporting" is enabled,	The Bayesian Engine will learn about messages the end user considers "spam."	Bayesian Engine performance will improve pertaining to the capture of potential spam messages.
Both options are enabled,	The Bayesian Engine will learn about both "ham" and "spam."	Performance will improve with regard to both false positives and false negatives.

Note: For Bayesian Training to work properly, you must enable BOTH User Spam Reporting and End User Quarantine functions. Other scenarios will result in failure to train properly.

CipherTrust recommends that users enable both training methods to allow the highest effectiveness for Bayesian Filtering in their own environments.

Bayesian and ESP

Bayesian filtering returns a value between 0 and 100 points to ESP. The value is actually the calculated probability (0 to 1) multiplied by 100.

Values	The Bayesian probability ((0 - 1) x 100) Confidence value: a pre-configured percentage
Formula	ESP Contribution = Bayesian probability X Confidence %
Example	Bayesian probability = .68 x 100 = 68 Confidence values = 20% ESP Contribution = 68 x 20% = 13 points.

Profiling Spam

Enterprise Spam Profiler

IronMail's Enterprise Spam Profiler allows the Administrator to achieve a high level of spam protection while keeping false positives to a minimum. Prior to ESP, spam-fighting tools were limited; no matter how many detection techniques were present, they all acted independently. IronMail uses a broad array of detection tools to analyze messages for spam. Then Enterprise Spam Profiler (ESP) aggregates the results of these multiple tools to calculate the probability that a message is spam. The result is much more trustworthy than the result from any spam detection tool alone.

IronMail provides two methods of spam-detection:

- *Tool-based spam detection* is based on emails being processed sequentially by each enabled spam-blocking tool. Once an individual tool thinks a message is spam, the specified action is taken and no other tools examine it. If ESP is not enabled, IronMail defaults to *tool-based spam detection.*
- *Confidence-based spam detection*, on the other hand, is based on having all enabled spam-blocking tools examine a message. Email is not considered spam until all spam

tools have each returned their respective determination regarding whether or not a message is spam. Each tool is "weighted" by the IronMail administrator as to its reliability in detecting spam, and returns a "probability score" for each message. ESP polls the individual enabled tools, then adds together each tool's probability score and takes an action only if the aggregate score reaches or exceeds an administrator-defined threshold. *Confidence-based spam detection* is enabled and configured in the Enterprise Spam Profiler page. If the Enterprise Spam Profiler is enabled, it enables *every previously enabled* spam-blocking tool to inspect the message

Note: Realtime Blackhole Lists (RBL), System Defined Header Analysis (SDHA) and User Defined Header Analysis all contribute scores to ESP based on rules triggered for each tool. No weighted averages are required for them.

ESP Profile

The ESP profile is the result calculated from the contributed scores from all enabled spam detection tools.

The following spam detection tools may contribute scores for the ESP profile:

- Reverse DNS (RDNS)
- Realtime Blackhole Lists (RBL)
- Statistical Lookup Service (SLS)
- System Defined Header Analysis (SDHA)
- User Defined Header Analysis (UDHA)
- Sender Policy Framework Lookup (SPF)
- Bayesian Filtering
- Content Filtering (Dictionaries)
    - Porn
    - Confidential
    - Spam
    - Malicious Mobile Code
    - URL
    - Bayesian Word List

    Other dictionaries may be added by the user if desired.

The Administrator can determine which tools and which dictionaries contribute to the profile. This is configured at Anti-Spam > Enterprise Spam Profiler > Configure.

Calculating the ESP Profile

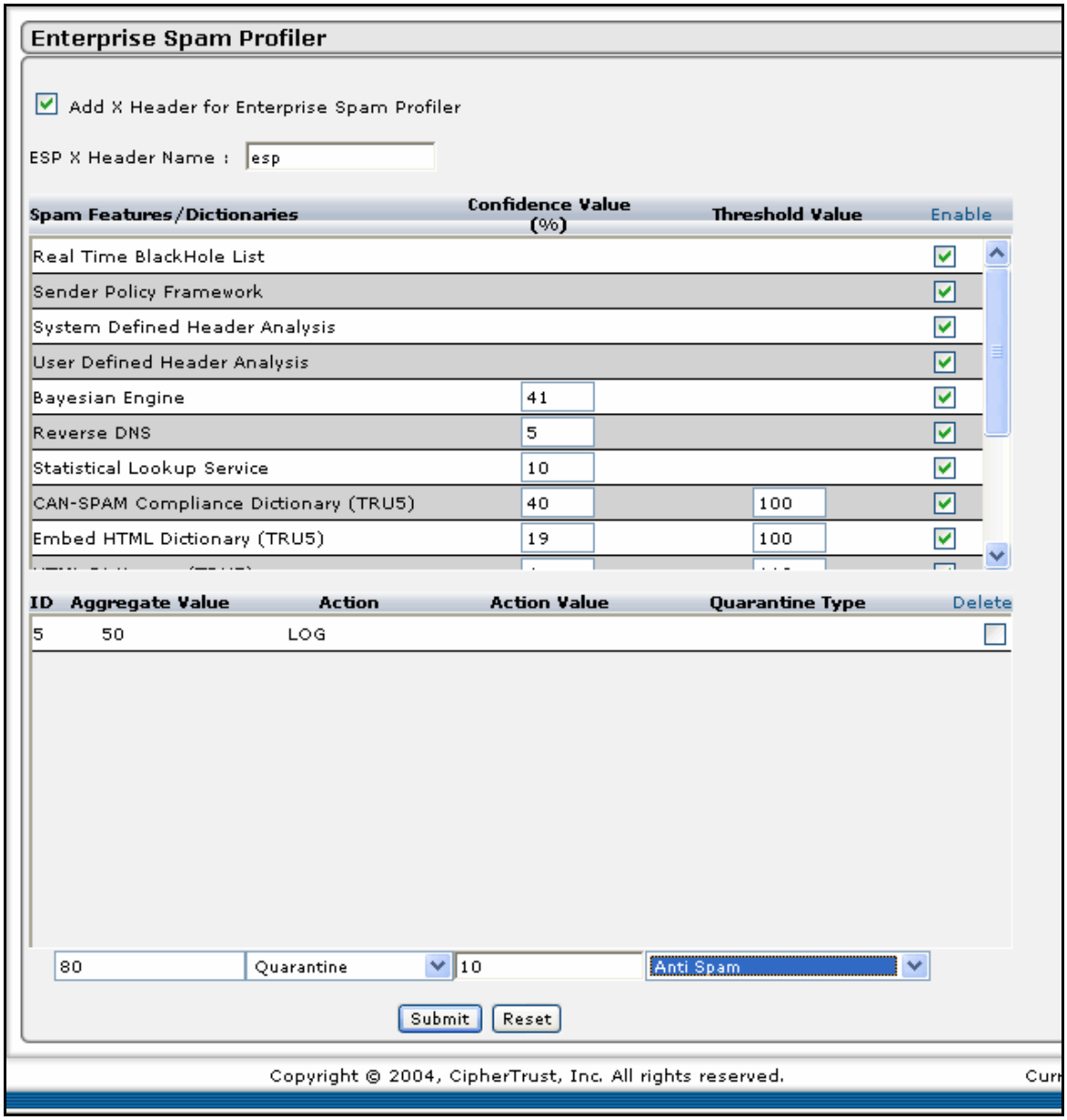
ESP can receive contributions from Content Filtering and many of the Anti-Spam tools. These contributions are totaled to calculate the aggregate value used as the ESP Profile. The contributions are identified in the table below.

Tools	Components	Detail
Reverse DNS	**Values**	No PTR record found: 100 pts. PTR record found: 0 pts. Confidence Value: a pre-configured percentage.
	Formula	ESP Contribution = RDNS value x Confidence %
Realtime Blackhole Lists	**Values**	Specific point values assigned to each zone in the list; positive numbers for blacklist entries, and negative numbers for whitelist entries.
	Formula	ESP Contribution = Sum of all matched RBL zone points.
Statistical Lookup Service	**Values**	SLS value based on a predetermined curve. Confidence Value: a pre-configured percentage.
	Formula	ESP Contribution = SLS value X Confidence %
System-Defined Header Analysis	**Values**	The configured point value for each triggered SDHA filter.
	Formula	ESP Contribution = Sum of all matched SDHA filter points.
User-Defined Header Analysis	**Values**	The configured point value for each triggered UDHA filter.
	Formula	ESP Contribution = Sum of all matched UDHA filter points.
Sender Profile Framework	**Values**	SPF lookup values (points).
	Formula	ESP Contribution = SPF lookup value points.
Bayesian Filtering	**Values**	The Bayesian probability ((0 - 1) x 100) Confidence value: a pre-configured percentage
	Formula	ESP Contribution = Bayesian probability X Confidence %
Content Filtering	**Values**	Point Score: individual word scores summed to generate a total point score. Threshold: the configured point value at which a message triggers CF rules.
	Formula	Confidence Value: a pre-configured percentage ESP Contribution = (Point Score/Threshold) X Confidence % In the formula, the threshold value acts as a ceiling limit for the point score so that the value is capped at the threshold value. The Point Score/Threshold can never exceed 100%.

Configuring ESP

Navigate to the ESP screens by starting IronMail and clicking on the Anti-Spam tab. Expand Enterprise Spam Profiler and click "Configure."

All IronMail spam-blocking tools display in the Enterprise Spam Profiler Configuration screen.


Enterprise Spam Profiler
Add X Header for Enterprise Spam Profiler
ESP X Header Name : esp
Spam Features/Dictionaries
Confidence Value (%)
Threshold Value
Enable
Real Time BlackHole List
Sender Policy Framework
System Defined Header Analysis
User Defined Header Analysis
Bayesian Engine 41
Reverse DNS 5
Statistical Lookup Service 10
CAN-SPAM Compliance Dictionary (TRU5) 40 100
Embed HTML Dictionary (TRU5) 19 100
ID Aggregate Value Action Action Value Quarantine Type Delete
5 50 LOG
80 Quarantine 10 Anti Spam
Submit Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

Administrators must assign a numeric confidence value to each tool. The weight represents, on a scale of 1 to 100, how confident the Administrator is that the tool successfully identifies spam without generating false positives. For example, administrators may conclude that SLS is 99% reliable, as long as there is no concern that newsletters are being stopped. If newsletters are a concern, then the confidence value for SLS might drop to 90%. Alternately, reverse DNS might be given a confidence value of only 40% because it can't know which legitimate domains have chosen not to configure reverse DNS. Once individual tools have been "weighted," Enterprise Spam Profiler policies are created by establishing actions that IronMail should take when certain point aggregate thresholds are reached.

The upper portion of the screen displays the following:

Field	Description
X-Headers	Click the check box to configure IronMail to add an X-header to the subject line of any message determined to be spam by the Enterprise Spam Profiler. Enter the text for the header in the data entry field.
Spam Features/Dictionaries	This column displays all of IronMail's spam-blocking tools that are processed within the Anti-Spam Queue.
Confidence Value	This column displays input fields in which the administrator must enter a measure of confidence for each tool. The numeric entry must be between 0 and 100. A "50" indicates that the tool can reasonably be expected to distinguish spam from legitimate email half the time. A value of "100" indicates total confidence that the tool will detect spam without any false positives. This may be understood as a way to weight the features to produce the expected result to trigger any threshold *rule*.
Threshold Value	This column displays the maximum point return thresholds for each applicable tool. The dictionaries return the number of points they find in the message. The threshold is the maximum number of points that will be considered to be 100%.
Enable	Select the **Enable** check box for each tool IronMail should use when performing confidence-based spam detection. It is expected that most administrators will enable all the spam tools. (Note that an anti-spam tool can be disabled here but still enabled within the tool's own configuration page.)

The lower portion is a table of Enterprise Spam Profiler policies containing the following information about each *policy* enabled:

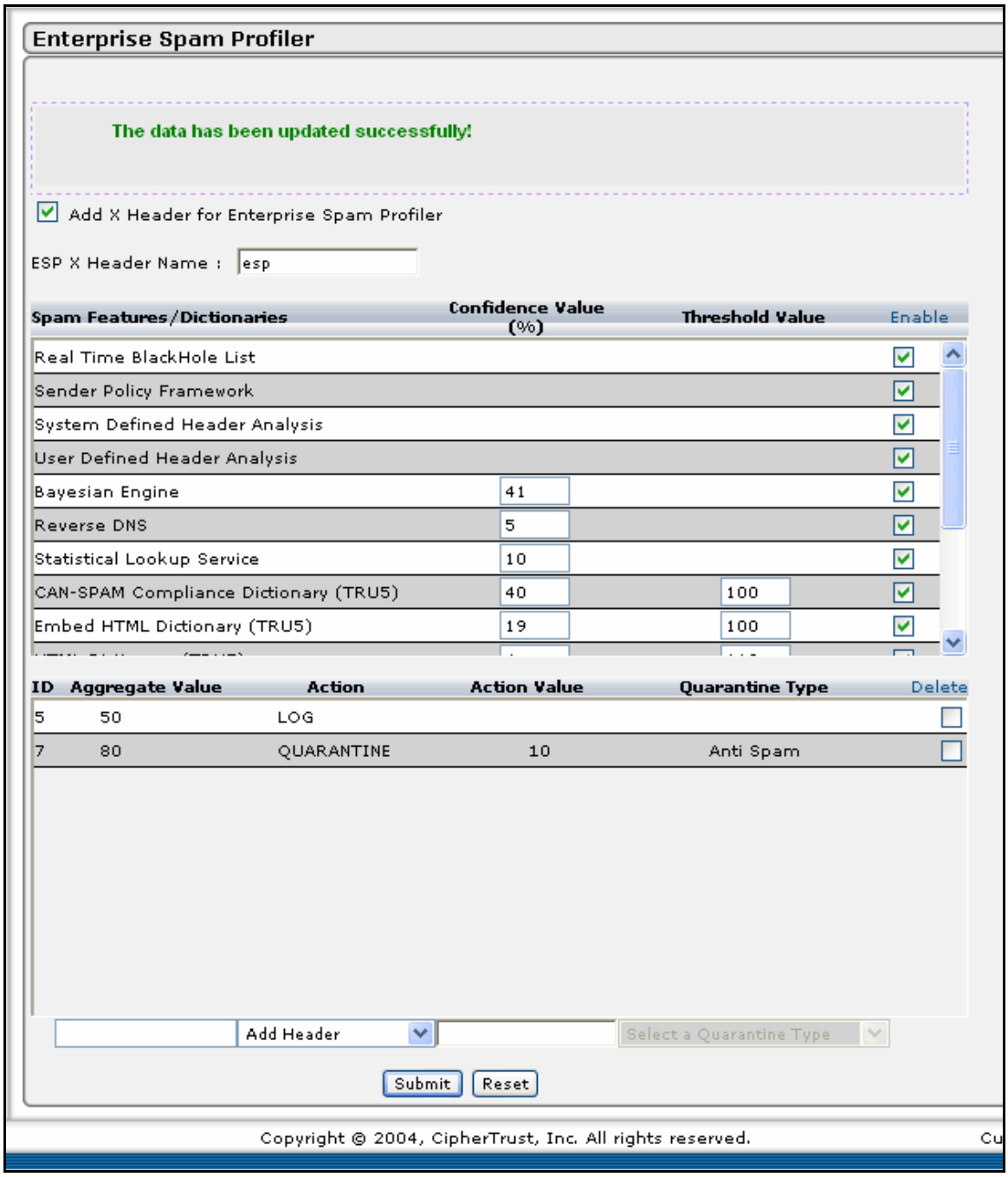
Field	Description
ID	This column contains the ID number for each specific policy.
Aggregate Value	This column displays the numeric threshold for each Enterprise Spam Profiler policy.
Action	This column displays the action IronMail should take when the associated threshold is reached.
Action Value	This column displays any data that qualifies the action.
Quarantine Type	If a quarantine action was specified, this column displays the name of the quarantine queue to which the message will be sent.
Delete	Select a policy's **Delete** check box and click **Submit** to delete an Enterprise Spam Profiler policy.

Below the table of Enterprise Spam Profiler policies are input fields used to create the policies:

Field	Description
Aggregate Value	Enter a number between 0 and 95 to represent the total calculated value for all contributing tools. If the sum of all spam tool calculations (the aggregate value) reaches this number, the action specified immediately to the right will be taken. For example, if the total confidence value is 50, an action is taken when the threshold of 50 is reached. The rule with the highest threshold value will apply.
Action	Select an action IronMail should take if an Enterprise Spam Profiler threshold is reached: • **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value input field below. For example, messages from the specified user, or with the specified Subject, can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the Action Data input field immediately below. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the Action Data field below. The forwarded message is rebound in the CipherTrust *MIME* boundary with an explanation of why it is forwarded. The original message is included as an attachment. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the Quarantine Type pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the Action Data field indicating how many days the message remains in the queue before being delivered out of the IronMail appliance. • **Log:** IronMail will deliver the message, but record in its SpamQ Detailed Log that the message matched a Spam rule. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** Enabling re-routing is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the Administrator must request Support to turn it on in the back end. Support will discuss the implications of enabling this action, allowing the user to make an informed decision about enabling re-routing. When it is enabled, the user will see the re-route action as part of the

	spam policy definitions.
Action Data	Some actions require qualifying information. • **Re-route:** this action requires a valid *IP address* of the SMTP host performing additional message processing. • **Quarantine:** this action requires a numeric value from 0 to 15. The number represents how many days the message will be quarantined before IronMail delivers it. For example, if a message is received at 12:30 PM on Wednesday and is quarantined for two days, IronMail will return the message to its regular mail flow at 12:30 PM Friday, and any queues that have not yet processed the message will do so before final delivery. A zero ("0") value, however, indicates "Do Not Deliver!" Any message in quarantine will be automatically deleted according to the Cleanup Schedule for "Quarantine Data" (*System > Cleanup Schedule*). • **Forward Message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. (If entering multiple email addresses, do NOT insert spaces after the commas.) • **Copy message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. (If entering multiple email addresses, do NOT insert spaces after the commas.) • **Subject Rewrite**:this action requires a text string that will IronMail will prepend to the message's Subject line. For example, messages from the specified user, or with the specified Subject, can have their Subject line prepended with the text "SUSPECTED SPAM!!!" • **Add Header:** A text string is required and must follow the RFC822 *protocol* rules for custom headers. The custom header format is: "**headername:headervalue**" where **headername** is an arbitrary name for the custom header, and **headervalue** is an arbitrary text string to display in the header. A sample custom header might be: "**X-HA-SPAM: 50**" ("**HA-SPAM**" is shorthand for "Header Analysis detected this message as SPAM," and "**50**" represents the policy's threshold. The header value string to the right of the colon cannot be longer than fifteen characters, and the custom header name may not contain a colon. (The colon is reserved as a delimiter between the header name and header value.)
Quarantine Type	If the Quarantine action is selected in the **Action** pick list to the left, this Quarantine Type pick list becomes enabled. It displays the default quarantine queues, and any other queues that were manually created. Select a queue where messages that reach the Aggregate Confidence threshold will be sent.

If the values on the configuration screen are satisfactory, click **Submit** to store the values.


Enterprise Spam Profiler
The data has been updated successfully!
Add X Header for Enterprise Spam Profiler
ESP X Header Name : esp
Spam Features/Dictionaries
Confidence Value (%)
Threshold Value
Enable
Real Time BlackHole List
Sender Policy Framework
System Defined Header Analysis
User Defined Header Analysis
Bayesian Engine 41
Reverse DNS 5
Statistical Lookup Service 10
CAN-SPAM Compliance Dictionary (TRU5) 40 100
Embed HTML Dictionary (TRU5) 19 100
ID Aggregate Value Action Action Value Quarantine Type Delete
5 50 LOG
7 80 QUARANTINE 10 Anti Spam
Add Header
Select a Quarantine Type
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

CipherTrust recommends accepting the default Enterprise Spam Profiler policy thresholds. If the confidence-based spam detection generates false positives, raise the Enterprise Spam Profiler threshold one point at a time until false positives no longer occur, or lower the individual spam-blocking tool's confidence values by one or two points at a time.

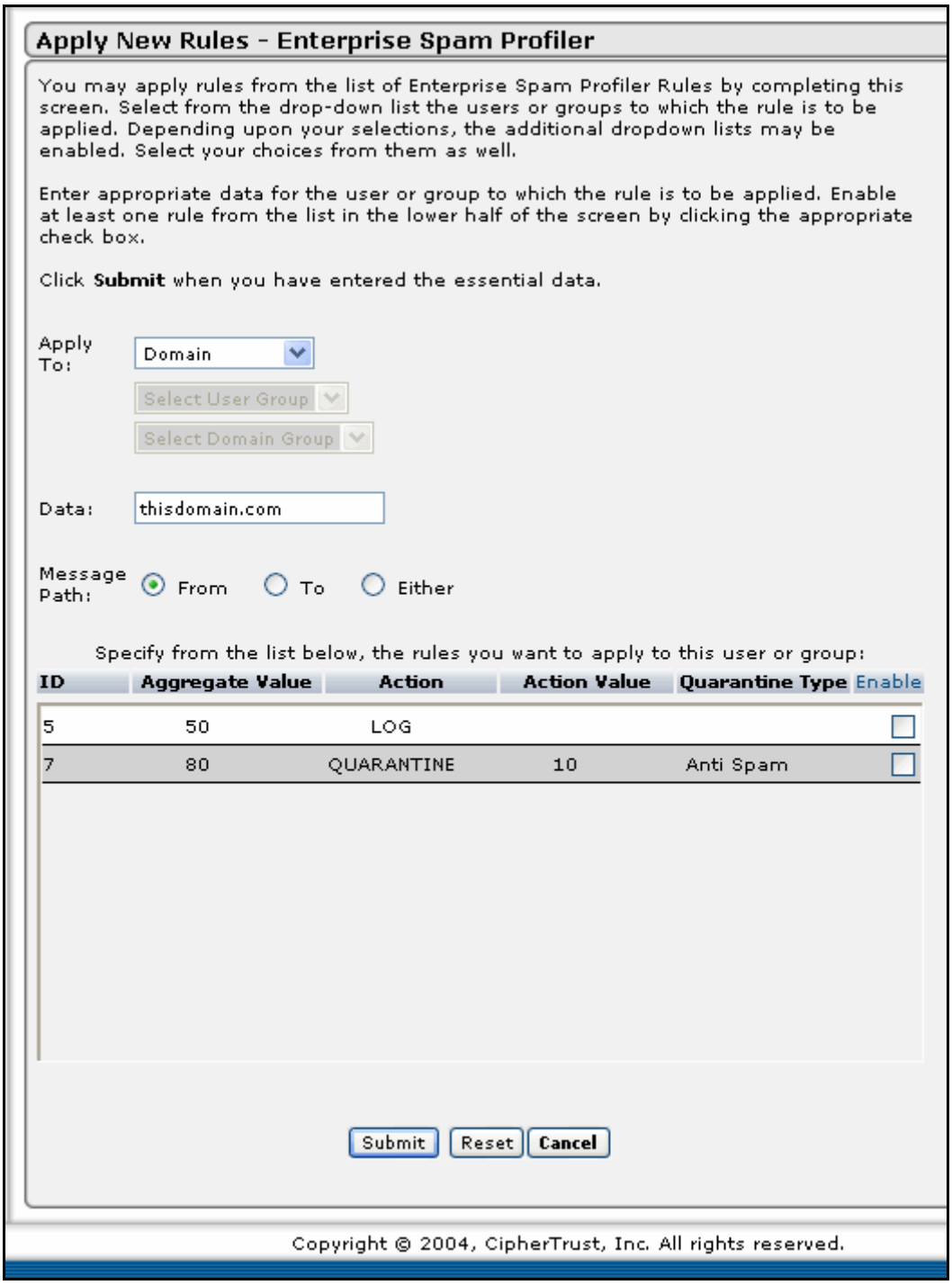
Applying ESP Rules

Click "Apply Rules" in the Anti-Spam menu. The Apply Rules - Enterprise Spam Profiler screen opens.

This screen allows the Administrator to view information about all the policies that are enabled for specific users and groups. You may add new policies by clicking the "Add New" button at the bottom of the screen. You may edit an existing *policy* by clicking the ID link for the policy you wish to change.

Adding ESP Policies

By clicking "Add New" on the Enterprise Spam Profiler Rules screen, the Administrator opens the screen for adding new rules.


Apply New Rules - Enterprise Spam Profiler
You may apply rules from the list of Enterprise Spam Profiler Rules by completing this screen. Select from the drop-down list the users or groups to which the rule is to be applied. Depending upon your selections, the additional dropdown lists may be enabled. Select your choices from them as well.
Enter appropriate data for the user or group to which the rule is to be applied. Enable at least one rule from the list in the lower half of the screen by clicking the appropriate check box.
Click Submit when you have entered the essential data.
Apply To:
Domain
Select User Group
Select Domain Group
Data:
thisdomain.com
Message Path:
From
To
Either
Specify from the list below, the rules you want to apply to this user or group:
ID
Aggregate Value
Action
Action Value
Quarantine Type
Enable
5
50
LOG
7
80
QUARANTINE
10
Anti Spam
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.

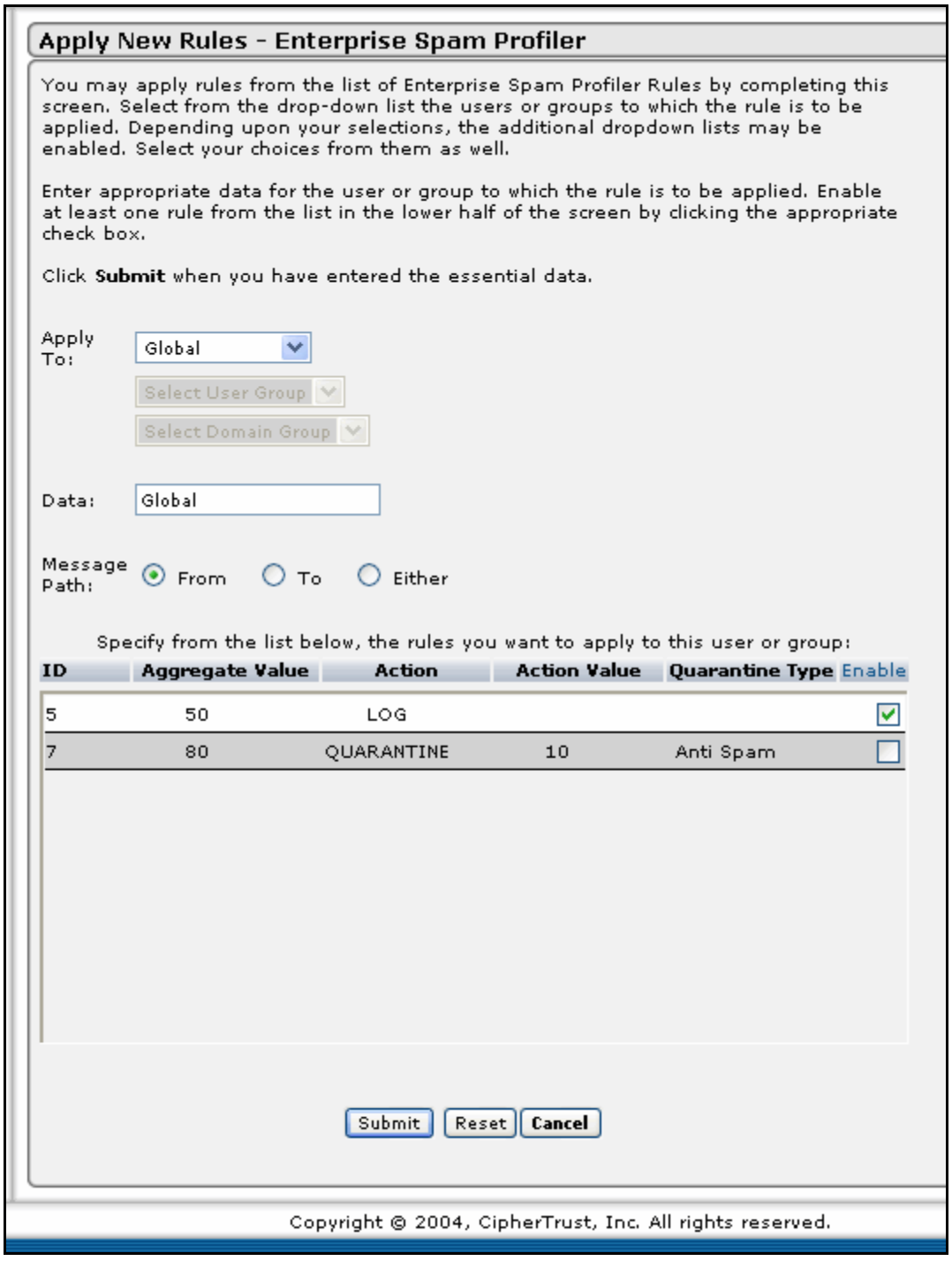
The screen contains the following information and data selections:

Field	Description
Apply To:	This field requires a selection from the drop-down list to determine if the rules are to be applied to everyone, or to a specific user or group. Some selections may enable additional drop-down lists that require additional choices.
Data	This field shows the result of the choice above.
Message Path	The radio buttons for the field allow you to choose the message direction (to, from or either) defining the messages to which the rules will be applied.
List of rules	***The table at the lower part of the screen provides information about all the available rules.***
ID	This column displays the system-generated ID number for the *rule* that may be applied.
Aggregate Value	The column shows the total value (threshold) at which the rule will be triggered. If a message accumulates the number of points specified, the designated action will occur.
Action	The configured action for each rule displays in this column.
Action Value	If the particular action calls for an associated value (e.g., number of days for the message to remain in quarantine), the configured value shows in this column.
Quarantine Type	If "Quarantine" is the configured action, the associated quarantine queue displays.
Enable	Clicking the Enable check box and clicking **Submit** enables the specified rule. Clicking the Enable hyperlink enables all rules for this *policy*.

Click **Submit** to save the new policy.

Editing ESP Policies

Clicking the ID link for a specific *rule* on the Enterprise Spam Profiler Rules screen allows the Administrator to edit that rule. The following screen opens.


Apply New Rules - Enterprise Spam Profiler
You may apply rules from the list of Enterprise Spam Profiler Rules by completing this screen. Select from the drop-down list the users or groups to which the rule is to be applied. Depending upon your selections, the additional dropdown lists may be enabled. Select your choices from them as well.
Enter appropriate data for the user or group to which the rule is to be applied. Enable at least one rule from the list in the lower half of the screen by clicking the appropriate check box.
Click Submit when you have entered the essential data.
Apply To:
Global
Select User Group
Select Domain Group
Data:
Global
Message Path:
From
To
Either
Specify from the list below, the rules you want to apply to this user or group:
ID
Aggregate Value
Action
Action Value
Quarantine Type
Enable
5
50
LOG
7
80
QUARANTINE
10
Anti Spam
Submit
Reset
Cancel
Copyright © 2004, CipherTrust, Inc. All rights reserved.

This screen is pre-populated with the same information as the Add Rules screen. You may make changes to the data as required.

Field	Description
Apply To:	This field requires a selection from the drop-down list to determine if the rules are to be applied to everyone, or to a specific user or group. Some selections may enable additional drop-down lists that require additional choices.
Data	This field shows the result of the choice above.
Message Path	The radio buttons for the field allow you to choose the message direction (to, from or either) defining the messages to which the rules will be applied.
List of rules	***The table at the lower part of the screen provides information about all the available rules.***
ID	This column displays the system-generated ID number for the rule that may be applied.
Aggregate Value	The column shows the total value (threshold) at which the rule will be triggered. If a message accumulates the number of points specified, the designated action will occur.
Action	The configured action for each rule displays in this column.
Action Value	If the particular action calls for an associated value (e.g., number of days for the message to remain in quarantine), the configured value shows in this column.
Quarantine Type	If "Quarantine" is the configured action, the associated quarantine queue displays.
Enable	Clicking the Enable check box and clicking Submit enables the specified rule. Clicking the Enable hyperlink enables all rules for this *policy*.

Click **Submit** to save the changes.

User, Group and Domain ESP Policies

The administrator can define ESP policies with multiple thresholds for action based on user, group and domain. The order of precedence for these user types is:

1. User
2. User Group
3. Domain
4. Domain Group
5. Global

User types are also defined as senders or receivers of messages.

When the ESP score exceeds a minimum ESP threshold, the users are evaluated to see if they qualify for any policies and rules. The overall score is compared with the identified thresholds to decide what action is to be taken. If a message qualifies for more than one *policy* with different user types, policy precedence depends on the order shown above. If a message qualifies for more than one policy with the same user type, the action is taken according to the defined Spam Order.

CipherTrust Experience

There are countless variations on which spam tools detect spam, and the values they return as the “raw data” and “probability of spam.” CipherTrust provides

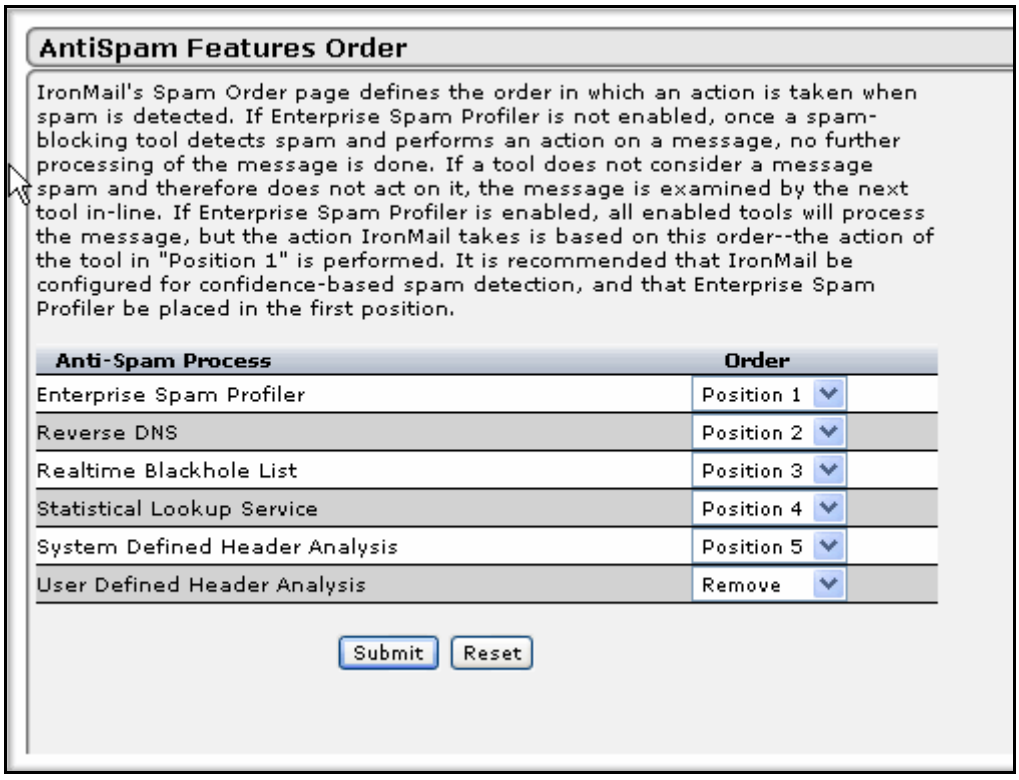
these thresholds based on its in-depth experience with spam and knowledge of IronMail's anti-spam capabilities. If IronMail's default thresholds ever generate false positives, either raise the Aggregate Confidence threshold here, or lower the confidence level for the spam-blocking tool that did not think the message was spam. It is recommended that values be decremented or incremented by "ones"—raise a threshold from 78 to 79, or lower a tool confidence-value from 50 to 49. Repeat as necessary.

Spam Order

IronMail's AntiSpam Features Order page defines the order in which an action is taken when spam is detected. Once an action is taken by any of IronMail's spam tools, no other spam action will occur. That is, if four of five of IronMail's spam-blocking tools determine that a message is spam, and their actions differ, IronMail will perform the action of the spam tool in the first position.

Ordinarily, Enterprise Spam Profiler should be placed in the first position, as it's spam-detection capability is more reliable than any other spam tool on its own. However, if Enterprise Spam Profiler is placed in a later position, then its action(s) will not be enforced unless all prior spam-blocking tools have declined to act on the message.

Bear in mind that unless Enterprise Spam Profiler is enabled, messages will not necessarily be evaluated by all of IronMail's spam-blocking tools—once a spam tool determines that a message is spam, no other tools evaluate it.


AntiSpam Features Order
IronMail's Spam Order page defines the order in which an action is taken when spam is detected. If Enterprise Spam Profiler is not enabled, once a spam-blocking tool detects spam and performs an action on a message, no further processing of the message is done. If a tool does not consider a message spam and therefore does not act on it, the message is examined by the next tool in-line. If Enterprise Spam Profiler is enabled, all enabled tools will process the message, but the action IronMail takes is based on this order--the action of the tool in "Position 1" is performed. It is recommended that IronMail be configured for confidence-based spam detection, and that Enterprise Spam Profiler be placed in the first position.
Anti-Spam Process
Order
Enterprise Spam Profiler
Position 1
Reverse DNS
Position 2
Realtime Blackhole List
Position 3
Statistical Lookup Service
Position 4
System Defined Header Analysis
Position 5
User Defined Header Analysis
Remove
Submit
Reset

All of the spam-blocking tools processed within the Anti-Spam Queue are identified on this page. For each enabled tool, a pick list allows the selection of an order. Selecting "Remove" instructs IronMail to not examine messages with that tool. Functionally, selecting "Remove" is the same as disabling the tool from within its own configuration page.

Reporting Spam

User Spam Reporting

Whenever spam is able to slip past IronMail's other spam-blocking tools (e.g., SLS, System Defined Header Analysis, etc.), User Spam Reporting is an effective "last line of defense." End users within the *network* may forward (as attachments) the spam that makes its way into their mailboxes to an email address that the IronMail appliance monitors. IronMail then allows the administrator to make Mail Monitoring policies that drop, quarantine, or take another action on future messages with the same message characteristics. While IronMail provides the option of automatically creating Mail Monitoring rules or requiring administrators to manually create the rules, CipherTrust encourages administrators to create these rules manually.

Note: Currently, User Spam Reporting is *incompatible* with GroupWise and Notes clients.)

The User Spam Reporting page reports the RFC822 header data. This information, from the User Spam Reporting table, can be used to create additional rules for blocking this same type of spam in the future without preventing the delivery of legitimate email.

Note that if User Spam Reporting is configured to automatically generate a Mail Monitoring *policy*, the policy will be identified as "system-generated" (an "X" will be displayed in the System column of the Mail Monitoring policy table). System-generated policies may not be deleted until all the individual Mail Monitoring rules used by that policy are deleted.

User Spam Reporting
Select Enable Spam Blocking to enable End User Spam reporting and blocking. Select Manual to manually create Spam-blocking rules based on enduser-forwarded email. Select Auto to automatically create a Spam-blocking rule based a reported message's MailFrom, Subject line, and IP address. Select Require End User Valid Subnet to force IronMail to only accept forwarded spam from users within a subnet that appears in the Allow Relay List (Mail Firewall > Allow Relay).
Setting
Enable Spam Blocking
Require End User Valid Subnet
Auto - automatically generate the Spam-blocking rules
Manual - manually configure Spam-blocking rules.
Spam notification address
euspam@x3.ctqa.net
Type Basis
Subject
Action
Forward Message
Quarantine Type
Anti Spam
Action Data
me@mydomain.com
Submit
Reset

The following configuration options display at the top of the End User Spam Reporting window:

Field	Description
Enable Spam Blocking	Select the **Enable Spam Blocking** check box to turn on end user spam reporting. When enabled, end users may forward (as attachments) any spam they receive in their mailboxes to the email address that IronMail monitors. (The email address is provided in the input field below.) Messages must be forwarded as attachments, not forwarded using the Forward button in the mail client. When forwarded at an attachment, the email client creates a new "message envelope" (the RFC821 header) and does not overwrite the RFC822 header of the attached spam. IronMail parses the message for the RFC822 information. If messages are simply forwarded,

	IronMail will be unable to extract the information about the spam, and will drop the message without taking any action. End users are not notified that their forwarded message was dropped. In Microsoft Outlook, users should create a new email addressed to the email address IronMail monitors, and drag the spam from their inbox into the body of the new message. When the spam is added in this way, it is an attachment. In Microsoft Outlook Express, right-click on a spam in the Inbox and select the option "Forward as attachment."
Require End User Valid *Subnet*	Select the **Require End User Valid Subnet** check box to instruct IronMail to only accept forwarded spam from users within the network. This prevents users outside the network from mischievously or malevolently submitting valid email addresses for blocking. If enabled, IronMail will not accept any message that does not originate from an *IP address* or subnet listed in the *Mail-Firewall > Allow Relay* table. (If this option is enabled, administrators should add to the Allow Relay table any internal IP subnets used within the enterprise so users may forward spam to the IronMail.)
Auto	When selected, IronMail will automatically generate Mail Monitoring rules based on an administrator-specified message characteristic. This is NOT the recommended configuration!
Manual	When selected, administrators must manually generate Mail Monitoring rules based on message characteristics of the spam that users forward to the IronMail. This is the recommended method.
Spam Notification Address	Enter a unique email address not used by any mail server in the domain. The username is arbitrary (but should be easy to remember—e.g. Spam@domain.com); the domain must be one that IronMail actually hosts. When messages are sent to the specified email address, IronMail will read the spam's From address, IP address (if it is present), and Subject line, and populate the table of forwarded spam with the data. **Note:** End users' email clients must be configured to send their messages to IronMail. If the clients are configured to send messages directly to a mail server, the mail server will drop the forwarded-as-attachments spam and IronMail will not receive or process them.
Type basis	The *rule* can be generated based on one of three message characteristics: • **IP:** the RFC821 From IP address. Note that spammers often remove the From IP address, so creating Mail Monitoring rules based on IP address may be less effective than rules based on Mail From or Subject. If a user forwards a spam that does not contain the RFC821 IP address, IronMail cannot create a rule that blocks messages from that source—spam from that source will continue to be allowed into the network. • **Mail From:** the RFC822 From email address. IronMail will perform an action whenever any message originates from the spam's email address. • **Subject:** The message's Subject line. IronMail will perform an action whenever any message contains the text string that appears in the spam's Subject line.
Action	Select an action that IronMail should take when messages with the IP or email address, or Subject line is received. Note that if IP address is selected, IronMail will only perform one action: Drop. For rules based on Mail From or Subject, select an action from the Action pick list:

	• **Subject rewrite:** IronMail will prepend the message's Subject line with a text string provided in the Action Value input field below. For example, messages from the specified user, or with the specified Subject, can have their Subject line prepended with the text "SUSPECTED SPAM!!!" A text string is required in the Action Data input field immediately below. • **Drop message:** IronMail will drop the entire message. • **Copy Message:** IronMail will deliver the original message but send a copy of the message as a file attachment within a new email addressed to the user specified in the Action Value column. (This is not a "BCC" or "blind copy" that is available in some email client applications.) • **Forward Message:** IronMail will forward the message to an alternate email address instead of the original recipient. When selected, a valid email address must be entered in the **Action Data** field below. • **Add Header:** IronMail will insert a custom RFC822 header, as specified in the **Action Data** input field below. The Add Header action is used primarily to allow other applications that have the ability to parse the RFC822 header to act upon any message that contains the custom header provided here. • **Quarantine:** IronMail will send the message to one of its quarantine queues. When Quarantine is specified as the action, the **Quarantine Type** pick list becomes enabled and the selection of a queue is required. (Any queue may be specified.) Additionally, a number must be entered in the **Action Data** field indicating how many days the message remains in the queue before being delivered out of the IronMail appliance. • **Log:** IronMail will deliver the message, but record in its SpamQ Detailed Log that the message matched a Mail Monitoring rule. • **Re-route:** IronMail will re-route messages to another IronMail appliance, rather than quarantining them. That appliance is dedicated to End User Quarantine; it will quarantine all messages and generate the EUQ notifications at a user-defined interval. The Administrator can then review a single report daily from that appliance to determine which senders should be whitelisted. **Note:** This is NOT the default configuration, and it cannot be set by the Administrator. To enable this option the installer must request Support to turn it on in the back end. When it is enabled, the user will see the re-route action as part of the spam policy definitions.
Quarantine Type	If the Quarantine action is selected in the **Action** pick list above, this **Quarantine Type** pick list becomes enabled. It displays the default quarantine queues, and any other queues that were manually created. Select a queue where messages detected by auto-generated spam-blocking rules will be sent.
Action Data	Some actions require qualifying information. • **Forward Message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered. • **Subject rewrite:** this action requires a text string. The text string may be any printable character up to 256 characters long. For example, Subject Rewrite can add the following text to the beginning of each message's Subject line: "SUSPECTED SPAM!!!" • **Copy message:** this action requires a valid email address. Multiple email addresses, separated by commas, may be entered.

	• **Re-route:** this action requires a valid IP address or machine name of the host performing additional message processing. • **Quarantine:** this action requires a numeric value from 0 to 15. The number represents how many days the message will be quarantined before IronMail delivers it. For example, if a message is received at 12:30 PM on Wednesday and is quarantined for two days, IronMail will return the message to its regular mail flow at 12:30 PM Friday, and any queues that have not yet processed the message will do so before final delivery. A zero ("0") value, however, indicates "Do Not Deliver!" Any message with a quarantine value of zero will be automatically deleted according to the Cleanup Schedule for "Quarantine Data" (*System > Cleanup Schedule*).

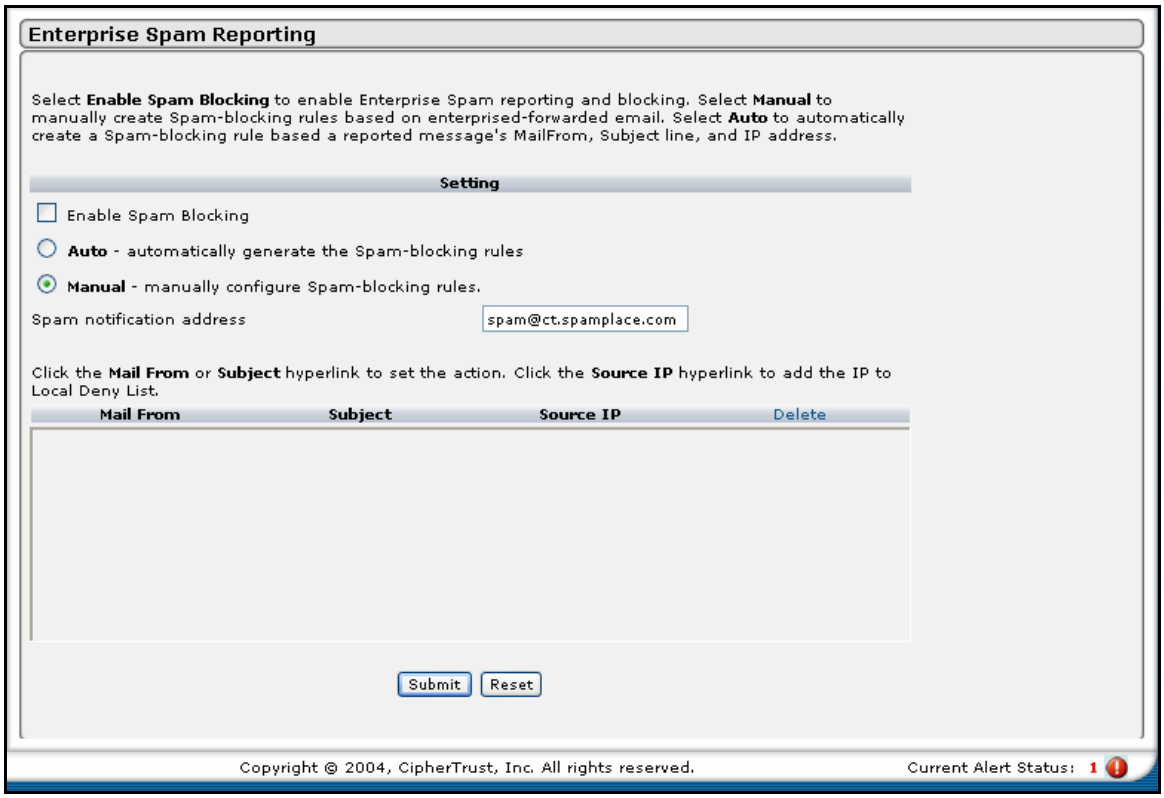
Click **Submit** after specifying an action and action value. The secondary window closes, and the User Spam Reporting page is refreshed. A "check" appears beside the address or Subject upon which a rule was just created. Messages for which a Mail Monitoring rule has already been created can be deleted. Select the message's **Delete** check box and click **Submit**. The message is deleted from the table of reported spam, not from Mail Monitoring's rules and policies.

Administrators are advised to "visit" End User Spam Reporting at least once a day to create Mail Monitoring rules for the reported spam. In large organizations, where many users are reporting spam, the table of reported spam can quickly grow, making the creation of rules for a week's worth of spam a daunting task.

Note: If end users configure their mail client to break large messages into multiple (smaller) messages, and they forward a large spam to IronMail, IronMail will be unable to parse and process the received spam. The message(s) will be dropped.

Enterprise Spam Reporting

Enterprise Spam Reporting functions similarly to End User Spam Reporting. The difference is that administrators will enter "honey pot" email addresses in the Spam Notification Address input field. That is, IronMail administrators may create fictitious email addresses for a domain that IronMail hosts, and submit these addresses to web sites and newsgroups where there is a high probability they will be acquired by spammers. (The username of the address must not be used by any internal mail server.) Spammers will begin sending their junk email and pornography to these addresses—addresses that IronMail will monitor. IronMail will populate the Enterprise Spam Reporting table of spam with those messages, and Mail Monitoring rules can be created for them.


Enterprise Spam Reporting
Select Enable Spam Blocking to enable Enterprise Spam reporting and blocking. Select Manual to manually create Spam-blocking rules based on enterprised-forwarded email. Select Auto to automatically create a Spam-blocking rule based a reported message's MailFrom, Subject line, and IP address.
Setting
Enable Spam Blocking
Auto - automatically generate the Spam-blocking rules
Manual - manually configure Spam-blocking rules.
Spam notification address
spam@ct.spamplace.com
Click the Mail From or Subject hyperlink to set the action. Click the Source IP hyperlink to add the IP to Local Deny List.
Mail From
Subject
Source IP
Delete
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 1

Enterprise Spam Reporting offers the following configuration options:

Field	Description
Enable Spam Blocking	Select the Enable Spam Blocking check box to turn on enterprise spam reporting. When enabled, spam mailed to the email address specified below will be read and "parsed" by IronMail, allowing the creation of Mail Monitoring rules to block those spams from entering the *network* in the future.
Auto	When selected, IronMail will automatically generate Mail Monitoring rules based on an administrator-specified message characteristic. This is NOT the recommended configuration.
Manual	When selected, administrators must manually generate Mail Monitoring rules based on a message characteristic of the spam that IronMail receives at the monitored address.
Spam Notification Address	Enter a unique email address not used by any mail server in the domain. The username part of the email address is arbitrary; the domain must be one that IronMail actually hosts. When messages are sent to the specified email address, IronMail will read the spam's From address, *IP address* (if it is present), and Subject line, and populate the table of forwarded spam with the data. Administrators may enter multiple email addresses, separated from each other with a comma.

Table of Submitted Spam	***The table lists all spam that has been submitted.***
Mail From	The spam's RFC822 From address is provided. The address is also a hyperlink. Clicking the hyperlink will allow administrators to create a Mail Monitoring *rule* based on the From address. (After submitting the rule, a "check" will be entered in the Select box beside the email address, indicating that a rule based on the address was created.)
Subject	The spam's Subject line is provided. The Subject is also a hyperlink. Clicking the hyperlink will allow administrators to create a Mail Monitoring rule based on the Subject line. (After submitting the rule, a "check" will be entered in the Select box beside the Subject, indicating that a rule based on the message's subject was created.)
Source IP	The spam's RFC821 IP address is provided. The address is also a hyperlink. Clicking the hyperlink will allow administrators to create a Mail Monitoring rule based on the IP address. (After submitting the rule, a "check" will be entered in the Select box beside the IP address, indicating that a rule based on the IP address was created.)
Delete	Select a forwarded spam message's **Delete** check box and click **Submit** to delete the message from this User Reporting Spam table. Deleting the message from this table does not delete any Mail Monitoring rules that may have been created based on one or more of its message characteristics.

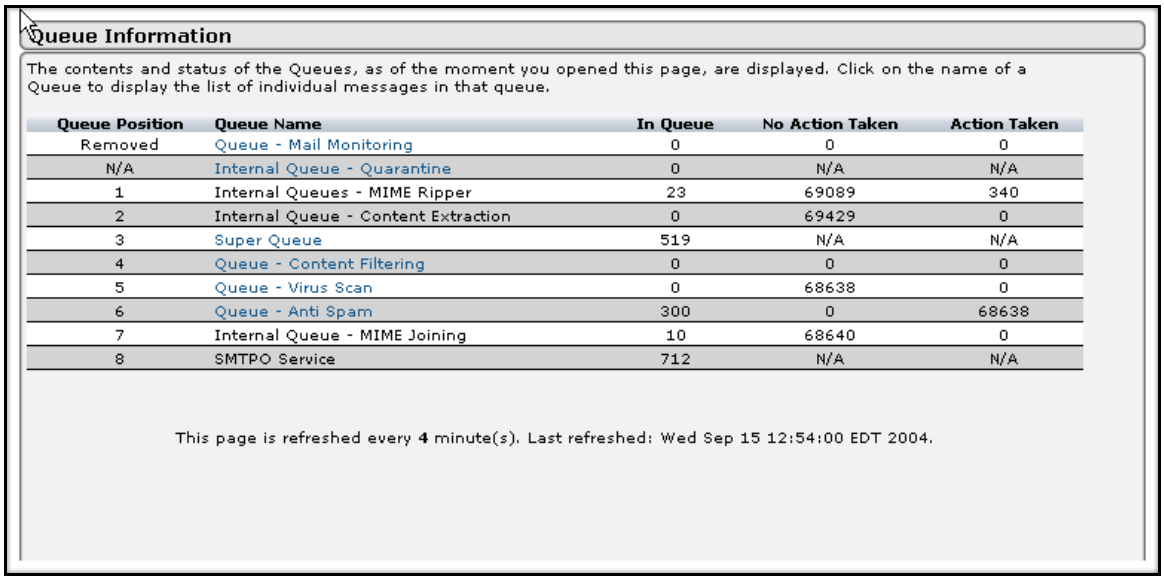
Administrators are advised to "visit" Enterprise Spam Reporting at least once a day to create Mail Monitoring rules for the reported spam. The table of reported spam can quickly grow, making the creation of rules for several days' or a week's worth of spam a daunting task.

To contribute to CipherTrust's goal of permanently solving the "spam problem," administrators may elect to forward all spam they receive at the Enterprise Spam Reporting address to CipherTrust, where CipherTrust's researchers and developers study them and search for ways to stop spam in the future. Navigate within IronMail's Web Administration interface to *Queue Manager > Configure Queues >* *Queue - Anti-Spam* > and select the "Enable global-stat report" option.

Queue Manager

Queue Information

The Queue Information page provides visibility into the current state of each of the queues. The Queue Information table displays how many messages are currently being processed within each queue, as well as other useful information. The data displayed in the table is static—each time the page is refreshed , the numbers of messages currently in the various queues change.


Queue Information
The contents and status of the Queues, as of the moment you opened this page, are displayed. Click on the name of a Queue to display the list of individual messages in that queue.
Queue Position | Queue Name | In Queue | No Action Taken | Action Taken
Removed | Queue - Mail Monitoring | 0 | 0 | 0
N/A | Internal Queue - Quarantine | 0 | N/A | N/A
1 | Internal Queues - MIME Ripper | 23 | 69089 | 340
2 | Internal Queue - Content Extraction | 0 | 69429 | 0
3 | Super Queue | 519 | N/A | N/A
4 | Queue - Content Filtering | 0 | 0 | 0
5 | Queue - Virus Scan | 0 | 68638 | 0
6 | Queue - Anti Spam | 300 | 0 | 68638
7 | Internal Queue - MIME Joining | 10 | 68640 | 0
8 | SMTPO Service | 712 | N/A | N/A
This page is refreshed every 4 minute(s). Last refreshed: Wed Sep 15 12:54:00 EDT 2004.

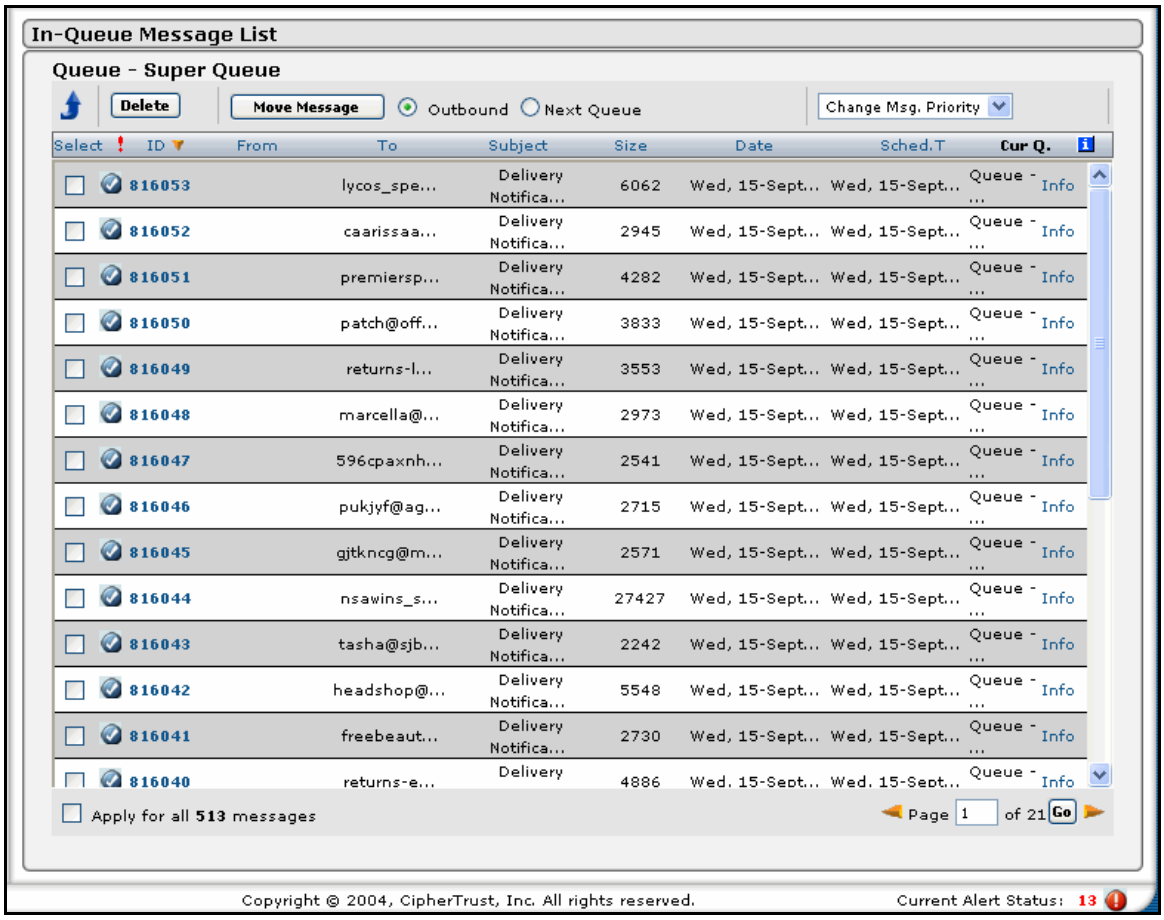
Note: The recommended way to manually refresh the Queue Information window (or other IronMail window) is to click on the associated menu option or hyperlink. Refreshing the window using the browser Refresh button can cause IronMail to logout.

The table displays the following information:

Field	Description
Queue Position	This column identifies the "queue position." Administrators may configure the order in which IronMail's queues process messages. The column will display a number representing the queue order, or the word "Removed" if a queue was removed from the message flow. The text "N/A" (Not Applicable) displays for the Quarantine Queue because it does not process messages. As each new message enters the appliance, IronMail notes which queues are to process the messages, and in which order. The Queue Position persists while the message traverses the queues. If the Queue Positions change after a message has entered the appliance, the new queue positions do not affect it; only messages received after the order was changed are affected.
Queue Name	This column identifies the name of the queue. Note that one row in the Queue Information table identifies the Quarantine Queue. When an IronMail *policy* sends a message to a specific system or user-defined quarantine queue, that subordinate queue's name will be displayed. Each queue's name is also a hyperlink that opens a secondary Message Header window. The secondary window displays detailed information about each message currently in that queue, and from which administrators may perform administrative tasks on them. When clicking a subordinate quarantine queue, the resulting Message Header window displays only the messages that were sent to that specific queue. If the parent Quarantine Queue hyperlink is clicked, the secondary window displays an unfiltered view of all messages that were

	quarantined. Note that when a queue name hyperlink is clicked, that queue pauses its processing of messages until the Message Header Details window is closed, five minutes of inactivity have lapsed, or IronMail's auto-refresh function releases queues that have been paused.
In Queue	This column displays the number of messages currently being processed in each queue as of the moment the Queue Information window was opened or refreshed. Note that the Quarantine Queue is a *logical* area of IronMail's Message Store. The number reported "In Queue" is the total of all messages that have been quarantined by any IronMail policy. The subordinate quarantine queues are filtered views of those messages, and report the number of messages in their respective queues.
No Action Taken	This column reports the cumulative total of messages processed within each queue for which IronMail did not perform an action based on a policy enforced by the queue. For example, if the Mail Monitoring queue processed 200 messages and enforced a policy that dropped three messages sent from user@domain.com, this column would display "197"—it did not take any action on 197 of the messages it processed. The numbers in this column are reset to zero when IronMail's Cleanup Schedule deletes the "Database Data" on its cleanup cycle (*System > Cleanup Schedule*).
Action Taken	This column reports the cumulative total of messages processed within each queue for which IronMail did perform an action based on a policy enforced by the queue. For example, if the Mail Monitoring queue processed 200 messages and enforced a policy that dropped three messages sent from user@domain.com, this column would display "3"—it took an action on 3 of the 200 messages it processed. The "Action Taken" value functions slightly differently within the quarantine queues. If an IronMail policy is designed to quarantine a message for two days, and the message is finally delivered, "no action is taken"—that message adds to the count in the No Action Taken column. If the IronMail policy declares that the message should be deleted on IronMail's Cleanup Schedule, the No Action Taken count will also be incremented accordingly. However, if the message is manually deleted, manually moved to another queue (including the Outbound Queue), or the message is forwarded to an alternate recipient, that action is added to the count in the Action Taken column. The numbers in this column are reset to zero when IronMail's Cleanup Schedule deletes the "Database Data" on its cleanup cycle (*System > Cleanup Schedule*).

When a "queue name" hyperlink is clicked, the In-Queue Message List for that queue displays, showing all messages waiting to be processed in that queue at the moment the List window opened.


In-Queue Message List
Queue - Super Queue
Delete
Move Message
Outbound
Next Queue
Change Msg. Priority
Select
ID
From
To
Subject
Size
Date
Sched.T
Cur Q.
816053 lycos_spe... Delivery Notifica... 6062 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816052 caarissaa... Delivery Notifica... 2945 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816051 premiersp... Delivery Notifica... 4282 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816050 patch@off... Delivery Notifica... 3833 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816049 returns-l... Delivery Notifica... 3553 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816048 marcella@... Delivery Notifica... 2973 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816047 596cpaxnh... Delivery Notifica... 2541 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816046 pukjyf@ag... Delivery Notifica... 2715 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816045 gjtkncg@m... Delivery Notifica... 2571 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816044 nsawins_s... Delivery Notifica... 27427 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816043 tasha@sjb... Delivery Notifica... 2242 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816042 headshop@... Delivery Notifica... 5548 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816041 freebeaut... Delivery Notifica... 2730 Wed, 15-Sept... Wed, 15-Sept... Queue - ... Info
816040 returns-e... Delivery 4886 Wed, 15-Sept... Wed, 15-Sept... Queue - Info
Apply for all 513 messages
Page 1 of 21 Go
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 13

The purpose of the Message List window is to provide administrators visibility into IronMail's queues, and to allow them to manually override IronMail's default actions. For example, administrators may delete messages, move them to alternate queues, view the message body, etc. (Messages that the queue has already begun to process are not displayed in the List window and cannot be deleted or otherwise "managed.") The Message List window is also useful for obtaining the Message ID before investigating messages listed in the Anti-Spam Queue Detailed Log.

The Message List window displays up to 20 messages at a time. If more than twenty messages are currently in the queue, a page number hyperlink is displayed at the lower right of the Message List window, allowing navigation to the next twenty messages. After navigating "forward" through one or more pages of messages, a **"Previous"** hyperlink is displayed, allowing backward navigation through the contents of the queue. Note that the messages visible in the Message Header table are statically displayed—messages that enter the queue *while the Message Header window is open* are not displayed until the Message Header window is closed and reopened again.

When the "**Apply For All *nnn* Messages**" check box at the bottom of the Message Header window displays a given number of messages, it is reporting the number of messages in that queue as of the moment the Message Header window was opened and that are viewable within this interface. To select all messages viewable within a domain's Message Header window without scrolling through the window one page at a time, select **Apply For All *nnn* Messages** at the bottom of the secondary browser window.

Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

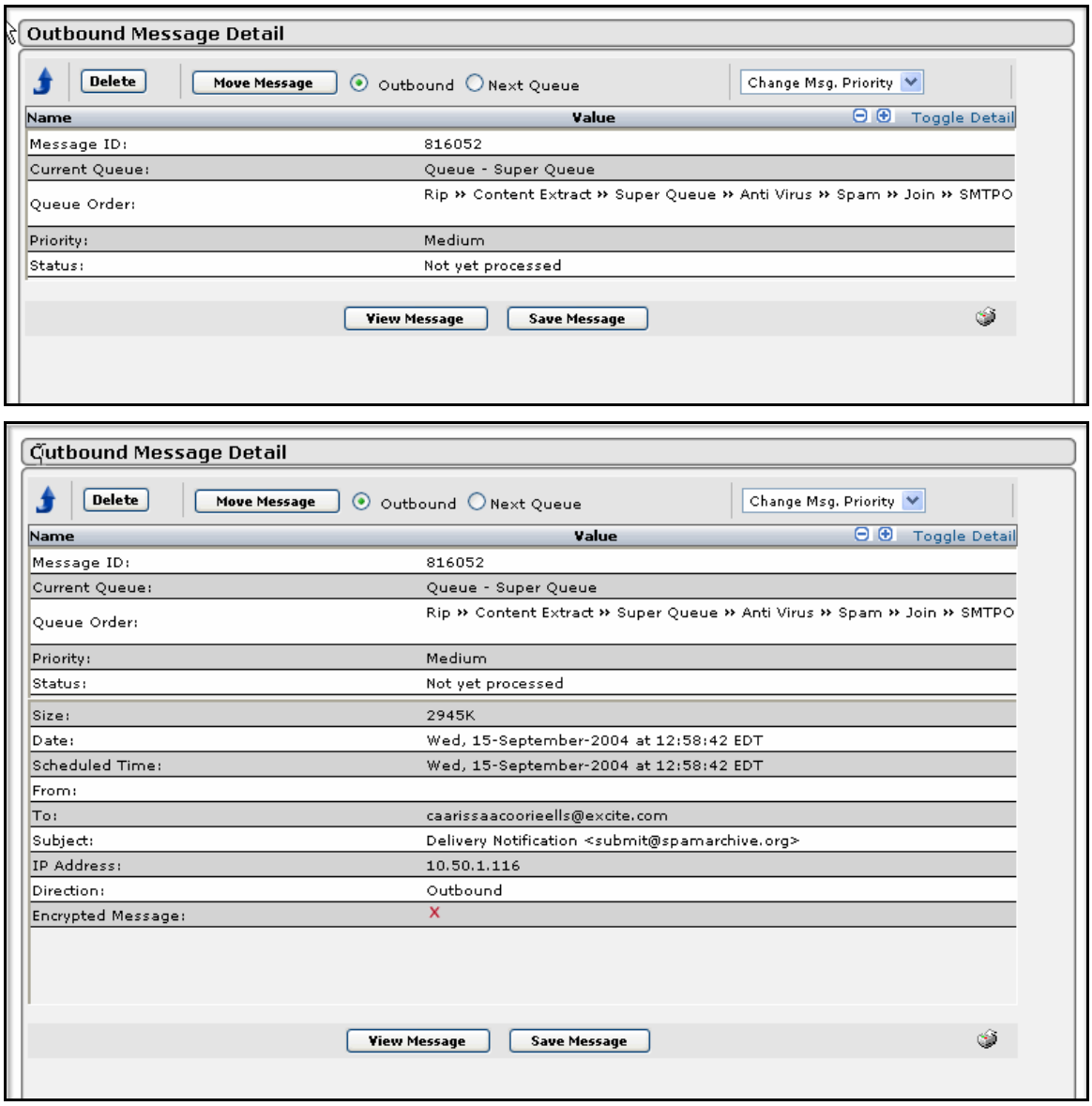
The Message List window displays the following information:

Field	Description
Delete	Click this button to delete all selected messages from the system.
Move Message	Click the proper destination button, then click the Move Message button to move all selected messages. Possible destinations are: • Outbound - moves all selected messages to IronMail's SMTPO Outbound Queue. They bypass any remaining queues that have not yet processed the messages. • Next Queue - move the message to the next queue in the processing order. This must be done one message at a time; batch moves are not supported.
Change Message Priority	From the drop down list, select the priority level for the message in question. Options are: • Highest • High • Medium (this is the default setting) • Low • Lowest
Select	A **Select** check box allows administrators to select one or more messages for administrative action. Clicking the **Select** column heading hyperlink selects all messages on the page. IronMail remembers messages that have been selected when administrators navigate through multiple pages. For example, if a message is selected on the first "page" of the Message Header window for the purpose of deleting it, and the administrator navigates two pages forward to select another message, both messages will be deleted when clicking the **Delete Message(s)** button at the bottom of the window. Alternately, the administrator may repeatedly click the **Select** column heading hyperlink on each page to select all messages on multiple pages for deletion or for movement to the Outbound Queue. To select all messages viewable within the Message Header window without scrolling through the window one page at a time, select "**Apply For All nnn Messages**" at the bottom of the secondary browser window. Note that while the secondary Message Header window is open, new messages may be entering the queue, even though message processing is temporarily paused. When this option is selected and an action is specified, the action does not apply to the newly-received, but not yet displayed messages.
ID	This column displays a number that uniquely identifies the message. The ID number is also a hyperlink that reveals details about the message. Detail screens are discussed below.
From	This column displays the RFC821 From address of the message sender. The From column heading is a hyperlink that sorts the Message Header table by From address in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened again.
To	This column displays the RFC821 To address of the message recipient. The To column heading is a hyperlink that sorts the Message Header table by To address in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened.

Subject	This column displays the message's Subject Line (which comes from the Subject in the RFC822 header). The Subject line is also a hyperlink that opens a tertiary Message Detail window displaying a variety of administrative actions that can be taken for the message. (See below.) Whereas only two actions are possible when selecting multiple messages (**Delete** and **Move to the Outbound Queue**), additional actions may be available through the tertiary window's interface when clicking the Subject of a single message: • The message priority may be changed. • The message may be moved to any other queue remaining to process it. • The message may be given a manually-assigned delivery date. • The message may be forwarded to an alternate email address. • The message header, body, and attachments may be viewed.
Size	This column displays the message's size. The Size column heading is a hyperlink that sorts the Message Header table by Size in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened again.
Date	This column displays the timestamp when each queue received the message. As a message traverses each queue, it will receive a new timestamp, anywhere from 1 to 60 seconds later than the previous timestamp, depending on IronMail's message load. (The Date column heading is a hyperlink that sorts the Message Header table by Date in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened again. Note that the quarantine queues have two times stamps: "Date" and "Schedule Time." The "Date" timestamp is when IronMail's SMTPI Service received the message. The "Schedule Time" timestamp is the delivery date based on the policy that sent the message to the quarantine queue. If a policy's action quarantines a message for two days, the "Schedule Time" will be two days after the SMTPI "Date." If a policy's action was to "not deliver" the message—i.e. a quarantine value of zero—the text "N/A" appears in the "Schedule Time column." A message's timestamp is a useful search parameter when searching for a message within each of IronMail's SMTPProxy logs—the log that record how IronMail processes the receipt of email.
Scheduled Time	This column shows the date and time the message was processed.
Info	Clicking the Info hyperlink for a message displays action details for that message. The detail screens will be discussed below.
Apply for all ___ messages	The check box associated with this field will apply the specified action to all the messages in the queue. The total number of messages that were present when the queue was opened displays.
Navigation	If multiple pages of messages exist for the current queue, navigation arrows and page numbers display at the lower right.

Message Details

Clicking the ID hyperlink for a message opens the Outbound Message Detail window. As the window first appears, only partial information is shown. If the Administrator needs more detail about the message, clicking the Toggle Detail hyperlink will display more information.

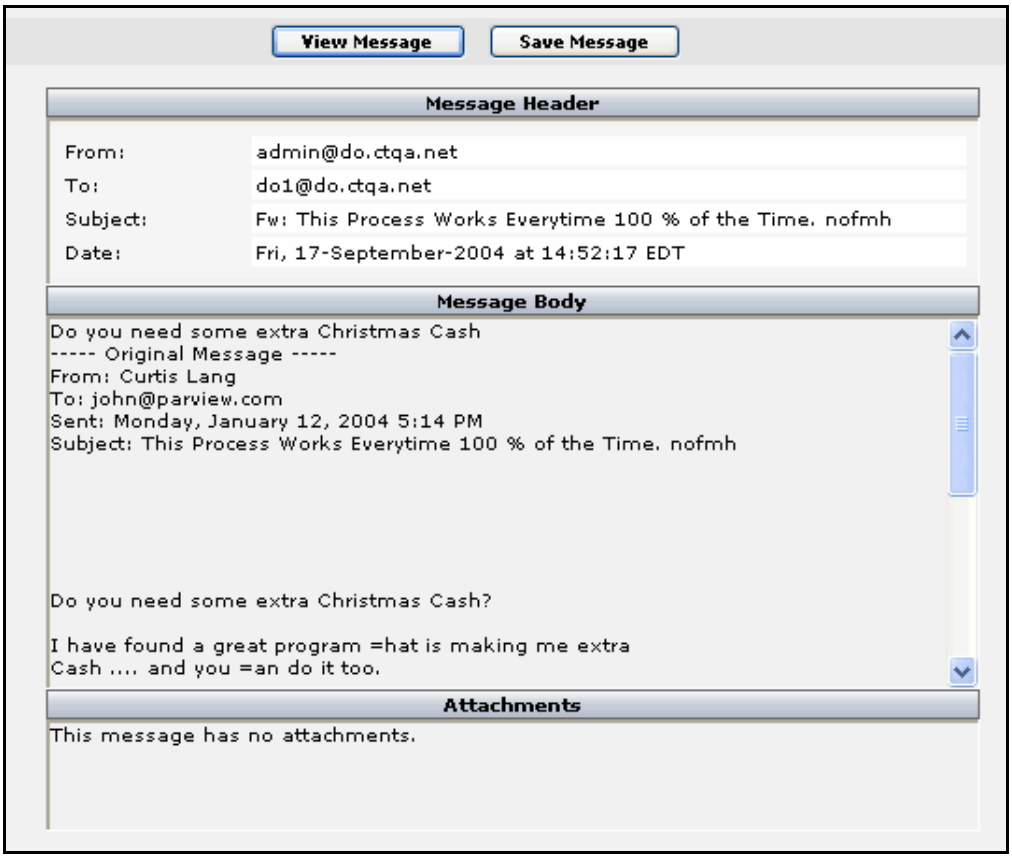


The Message Detail window provides the following:

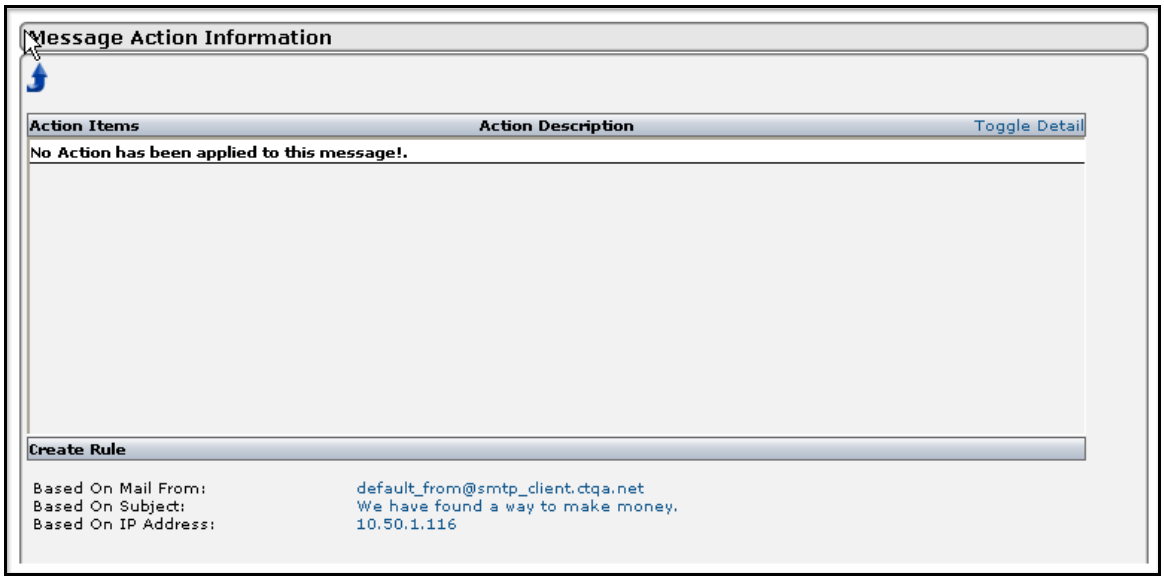
Field	Description
Delete	Click this button to delete all selected messages from the system.
Move Message	Click the proper destination button, then click the Move Message button to move all selected messages. Possible destinations are: • Outbound - moves all selected messages to IronMail's SMTPO Outbound Queue. They bypass any remaining queues that have not yet processed the messages. • Next Queue - move the message to the next queue in the processing order. This must be done one message at a time; batch moves are not supported.

Change Message Priority	From the drop down list, select the priority level for the message in question. Options are: • Highest • High • Medium (this is the default setting) • Low • Lowest
Name	This column lists all the information fields for which information is provided.
Value	This column shows the actual information from the selected message.
View Message	A **View Message** hyperlink opens a Message Viewer window in which the message's header, body, and file attachments may be viewed. When investigating whether a message that looks like a normal email is legitimate or really spam, view the message to confirm. **Note:** The view message function is not active in the case of *MIME* parse failure messages. **Note:** If the 822 message is HTML, the message body section will be blank.
Save Message	This button allows the Administrator to save and enact changes to the message.

The View Message button causes the message itself to display, should the Administrator need to see it.


View Message
Save Message
Message Header
From: admin@do.ctqa.net
To: do1@do.ctqa.net
Subject: Fw: This Process Works Everytime 100 % of the Time. nofmh
Date: Fri, 17-September-2004 at 14:52:17 EDT
Message Body
Do you need some extra Christmas Cash
----- Original Message -----
From: Curtis Lang
To: john@parview.com
Sent: Monday, January 12, 2004 5:14 PM
Subject: This Process Works Everytime 100 % of the Time. nofmh
Do you need some extra Christmas Cash?
I have found a great program =hat is making me extra
Cash .... and you =an do it too.
Attachments
This message has no attachments.

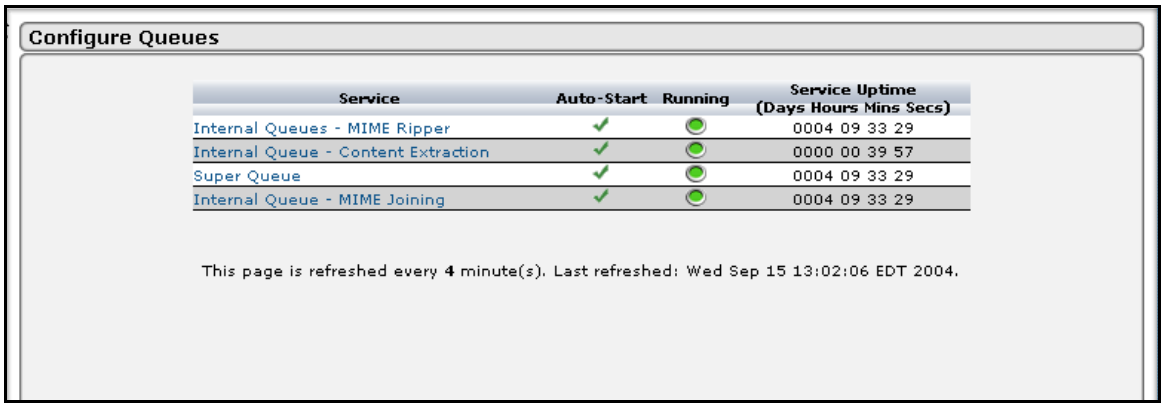
Clicking the Info hyperlink on the In-Queue Message List screen displays the Message Action Information where one can review any actions that IronMail has taken on the message.



Configure Queues

The Configure Queues page is used to stop and start queues, establish the order in which IronMail's queues process messages, and configure individual queue options.

The Configure Queues table displays the following information:

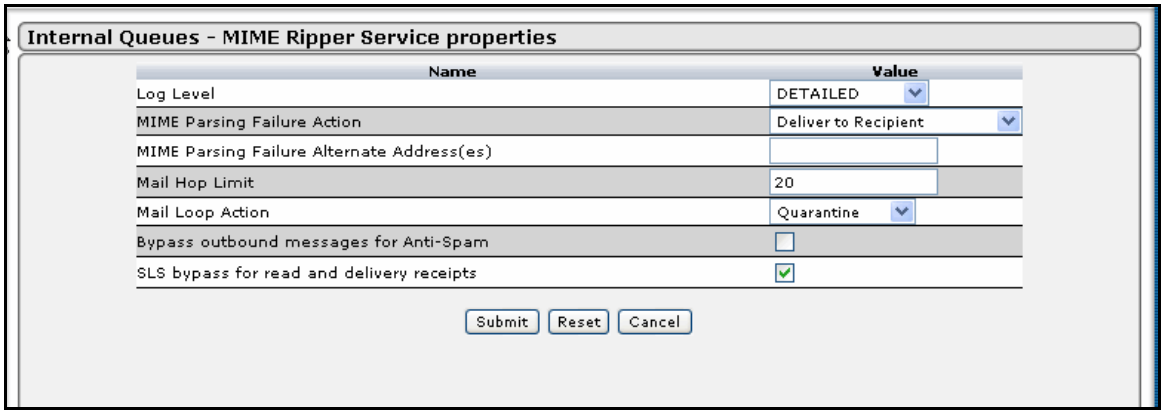

Configure Queues
Service
Auto-Start
Running
Service Uptime (Days Hours Mins Secs)
Internal Queues - MIME Ripper
0004 09 33 29
Internal Queue - Content Extraction
0000 00 39 57
Super Queue
0004 09 33 29
Internal Queue - MIME Joining
0004 09 33 29
This page is refreshed every 4 minute(s). Last refreshed: Wed Sep 15 13:02:06 EDT 2004.

Service	This column identifies the name of each queue. Each queue name is also a hyperlink that opens a secondary browser window displaying configuration options for that queue. The queues are: • **Internal Queues - *MIME* Ripper** • **Internal Queue - Content Extraction** • **Super Queue** • **Internal Queue - MIME Joining**
Auto-Start	This column displays one of two icons to indicate whether or not the queue is configured to start automatically when the IronMail appliance restarts. A green check indicates that the queue is configured to auto-start. A red X indicates that the queue is configured *not* to restart. Each icon is also a hyperlink that toggles the option on or off. **Note:** When a queue is configured to auto-start, IronMail's Health Monitor (a

	subsystem designed to continuously monitor the state of the IronMail appliance) will automatically attempt to restart a queue that has stopped for any reason. (A queue may stop due to a program error, or because an administrator temporarily stopped it manually.)
Running	This column displays one of two icons to indicate whether the queue is currently running or not. A green light indicates that the queue is currently running. A red light indicates that the queue is currently stopped. Each icon is also a hyperlink that toggles the queue on or off.
Service Uptime	This column displays, in days, hours, and minutes, how long the Queue Service has been running since it was last stopped.

Configuring MIME Ripper

Clicking the queue name in the service column of the Configure Queues screen opens a secondary window that allows configuration of that specific queue. The screen for the MIME Ripper is shown below.



Provide the following configuration information.

Name	Value
Log Level	Select a log level from the pick list. Options are: • Information • Error • Critical • Detailed
MIME Parsing Failure Action	Select the appropriate action from the drop-down list. Options are: • Drop Message • Deliver to Recipient • Deliver to Alternate Address • Quarantine
MIME Parsing Failure Alternate Address(es)	Enter the address (or addresses) to which messages that fail MIME parsing are to be sent.
Mail Hop Limit	Enter a number from 1 to 20 to represent the number of mail hops allowed before the message is received by IronMail.

Mail Loop Action	Select the appropriate action from the drop-down list. Options are: • Drop Message • Quarantine
Bypass outbound messages for Anti-Spam	Checking this checkbox enables outbound messages to bypass the Anti-Spam sub-queue processes.
SLS bypass for read and delivery receipts	Checking this checkbox enables read receipts and delivery receipts to bypass the SLS functionality.
Commands	Click the appropriate button: • Submit - writes changes to the database, executing changes • Reset - returns the screen to the state it was in when it opened • Cancel - closes the screen without saving any changes

Configuring Content Extraction

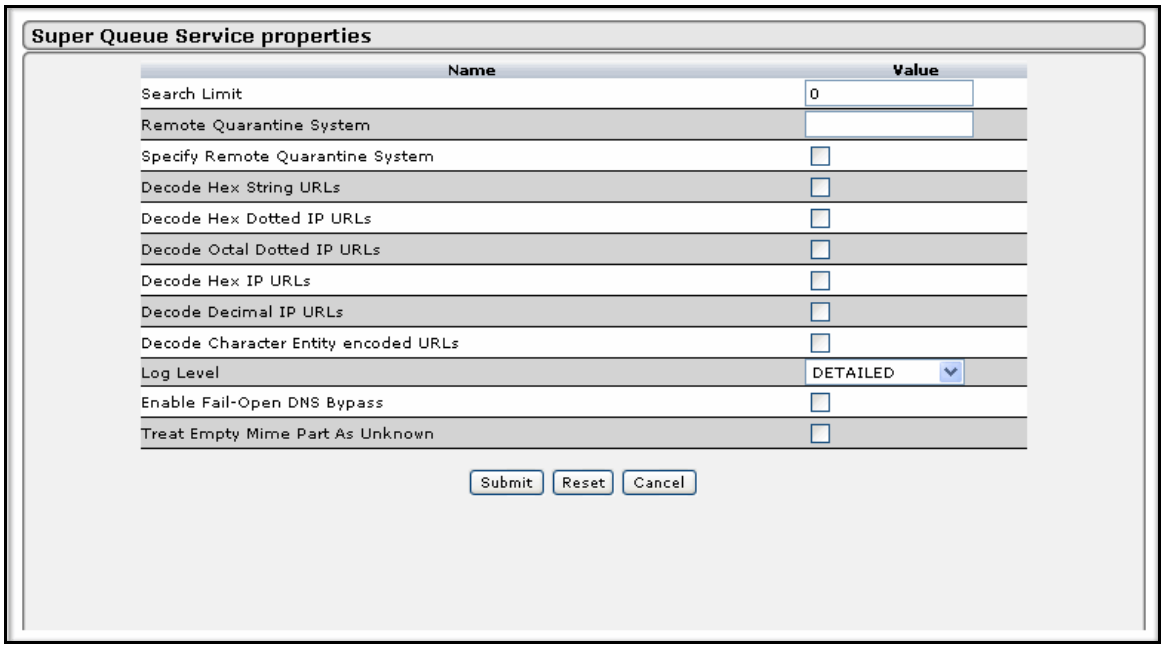
Clicking the queue name in the service column of the Configure Queues screen opens a secondary window that allows configuration of that specific queue. The screen for the Content Extraction queue is shown below.

Provide the following configuration information.

Name	Value
Log Level	Select a log level from the pick list. Options are: • Information • Error • Critical • Detailed
Commands	Click the appropriate button: • Submit - writes changes to the database, executing changes • Reset - returns the screen to the state it was in when it opened • Cancel - closes the screen without saving any changes

Configuring Super Queue

Clicking the queue name in the service column of the Configure Queues screen opens a secondary window that allows configuration of that specific queue. The screen for the Super Queue is shown below.



Provide the following configuration information.

Name	Value
Log Level	Select a log level from the pick list. Options are: • Information • Error • Critical • Detailed
Remote Quarantine System	Enter the hostname or IP address for the server to which quarantined messages are to be forwarded.
Specify Remote Quarantine System	Clicking the checkbox enables or disables the requirement to specify a remote quarantine system (Consolidated Quarantine Server).
Remote Quarantine System	
Search Limit	Enter a number to represent, in kilobytes, the portion of a message each feature is to scan. If no indications of spam, etc., are detected within this amount, the feature will stop processing and send the message on to the next feature.
Enable Fail-Open DNS Bypass	
Decode Hex String URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).

Decode Hex Dotted IP URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).
Decode Octal Dotted IP URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).
Decode Hex IP URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).
Decode Decimal IP URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).
Decode Character Entity encoded URLs	Checking this checkbox enables IronMail to decode URLs of this type (see table below).
Treat Empty MIME part as Unknown	
Commands	Click the appropriate button: • Submit - writes changes to the database, executing changes • Reset - returns the screen to the state it was in when it opened • Cancel - closes the screen without saving any changes

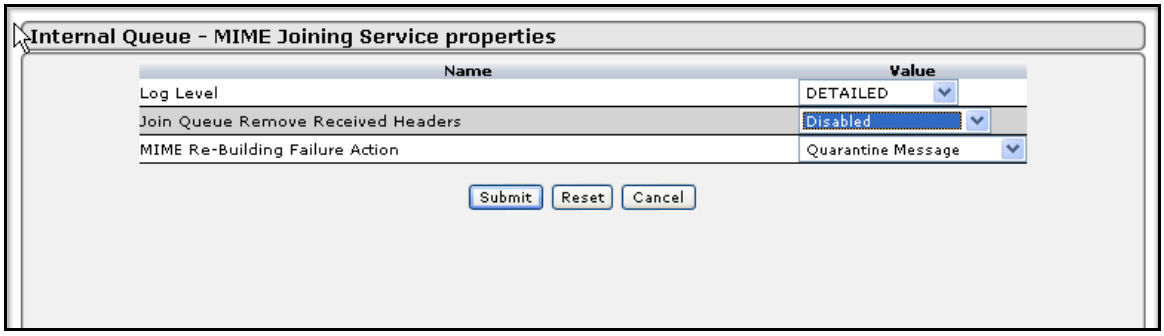
The encoded URLs that IronMail decodes are explained in the following table.

Encoding Type	Explanation
Hexadecimal string URLs	Spammers replace the letters in a URL with their equivalent hex code. When the user clicks on the link, the browser will decode the hex codes back to their original form. IronMail decodes the URL to see it in plain text, then finds it in the URL dictionary. **Example:** http://hotmail.com can be represented as: http://%77%77%77%2E%68%6F%74%6D%%61%69%6C%2E%63%6F%6D
Hexadecimal dotted IP URLs	Spammers encode the *IP address* in its hexadecimal form based on a calculation from the original IP address. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** the hexadecimal number for 207.178.42.40 is 0xCF.0xB2.0x2A.0x28, so http://207.178.42.40 can be represented as http://0xCF.0xB2.0x2A.0x28
Hexadecimal IP URLs	Spammers encode the IP address in its hexadecimal form as a non-dotted hex IP. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** http://207.178.42.40 can be represented as http://0xCFB22A28. It can be further obscured by adding an number of hexadecimal digits in front of the encoded URL, e.g., http://0x9AF0800CFB22A28
Decimal IP URLs	Spammers encode the IP address as a non-dotted decimal IP, based on a calculation from the original IP address. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** the calculated code for 206.159.40.2 is 3466536962, so http://206.159.40.2 can be represented as http://3466536962

Octal dotted IP URLs	Spammers represent the IP address in octal form, base 8. IronMail decodes the URL and finds it in the URL Dictionary. **Example:** http://207.178.42.40 can be represented as: http://0317.0262.052.050, or http://000317.0000262.00052.0050
Character Entity Encoded URLs	Spammers use this method to represent characters in the HTML document in one of three ways: • as decimal numbers • as hexadecimal numbers • as names, in some cases. Only a few characters have names, but any character may be represented by a decimal number or hex number. IronMail supports decoding of decimal representations of character entities. **Example:** http://www.hotmail.com can be represented as: http://www.hotmail.com

Configuring MIME Joinner

Clicking the queue name in the service column of the Configure Queues screen opens a secondary window that allows configuration of that specific queue. The screen for the MIME Joiner is shown below.



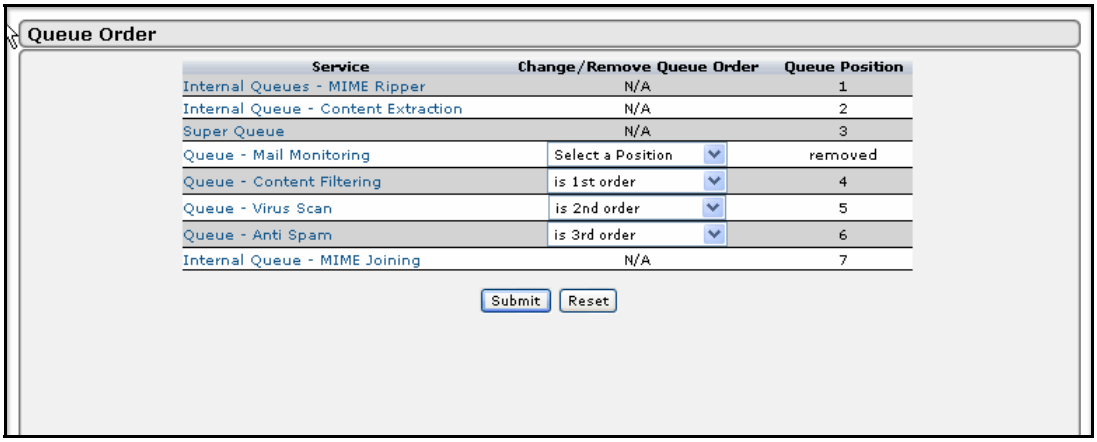
Provide the following configuration information.

Name	Value
Log Level	Select a log level from the pick list. Options are: • Information • Error • Critical • Detailed
Join Queue Remove Received Headers	Select a parameter from the drop-down list to enable the queue to remove RFC 822 headers from particular messages. The options are: • Disabled - turns off this functionality • All Messages - the queue will remove headers from both inbound and outbound messages • Inbound Messages - the queue will remove headers from inbound messages only

	• Outbound Messages - the queue will remove headers from outbound messages only
MIME Re-Building Failure Action	Select a parameter from the drop-down list to specify what IronMail will do if a message fails the rebuilding process. The options are: • Drop - drop the message • Quarantine - write the failed message to the Failures Queue • Deliver Original Message - retrieve the unparsed copy of the original message and deliver that to the recipient
Commands	Click the appropriate button: • Submit - writes changes to the database, executing changes • Reset - returns the screen to the state it was in when it opened • Cancel - closes the screen without saving any changes

Setting the Queue Order

This screen allows the Administrator to set the order of processing for the sub-queues within the Super Queue. The screen originally appears like this:



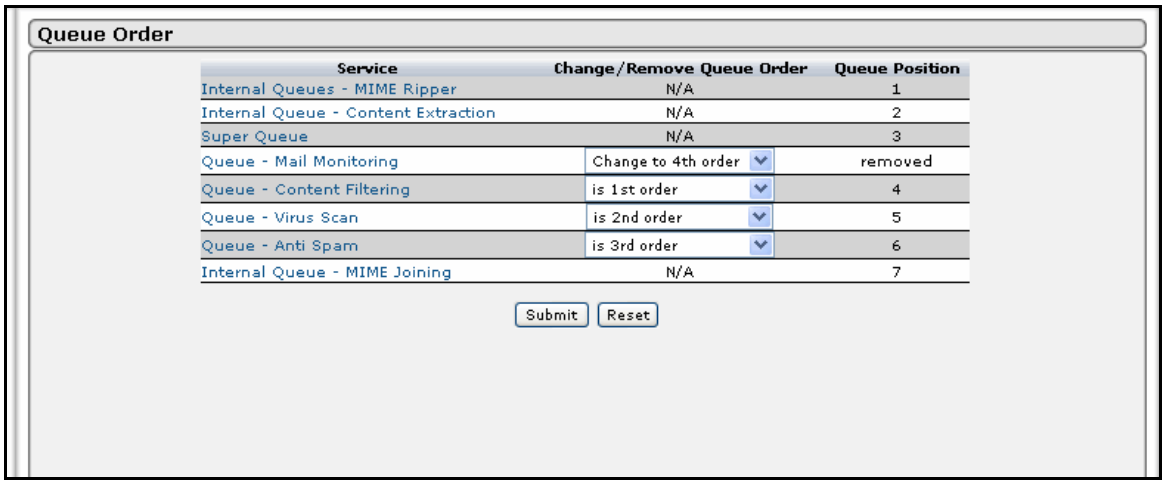
The Administrator may enable the available queues by setting their order.

Note: In network configurations that use a Consolidated Quarantine Server (CQS), the processing order, rules and policies must be configured the same way on all IronMail appliances. If this is not done, the CQS will not function properly.

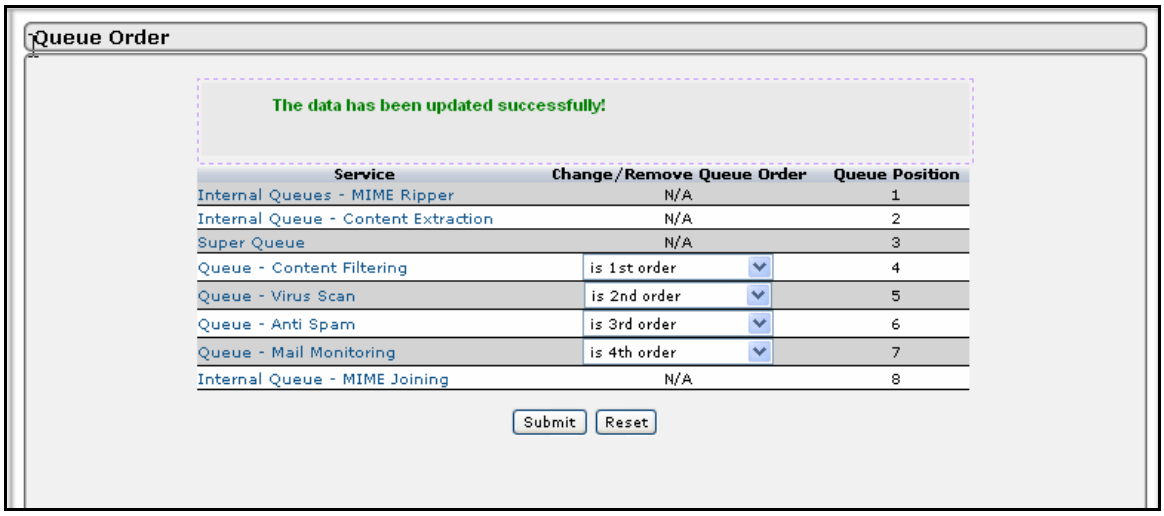
Column Name	Description
Service	This column lists the names of all the queues included in IronMail.
Change/Remove Queues Order	For each of the configurable sub-queues within Super Queue, this field contains a drop-down list that allows establishing the order in which the queues will process messages. The options are: • Remove - leave this sub-queue out of the processing order • Change to first position • Change to second position • Change to third position • Change to fourth position
Q Position	This field shows the processing order of all configured queues.

Changing the Order

The Administrator may change the queue order by selecting the desired change from the pick list. If a desired change will conflict with an existing setting, other changes must be enacted at the same time to define the complete order.



When the order has been established, click **Submit** to save the changes. The screen will refresh to show the order selected. And example showing a configured queue order appears below.



There are a variety of reasons why administrators may want to place IronMail's Queues in one order as opposed to another. Here are typical examples:

- Anti-Spam Queue **first**: If the Anti-Spam Queue is able to block 40% or more of all incoming messages, this greatly reduces the processing burden of the remaining queues.
- Virus Queue is **last**: The Anti-Virus Queue is the most CPU-intensive of all IronMail's queues. An argument can be made for *not* placing it in the first position, then. If all the queues preceding it can reduce the number of messages that finally get delivered to it, then some CPU cycle time is saved.
- Virus Queue **first**: Though the Anti-Virus Queue in the first position will not, by definition, provide any CPU-savings, it ensures that *every message* gets scanned for viruses. If the Anti-Virus Queue is placed last, there is always the chance that administrators may

unwittingly push an infected out of the Quarantine Queue (sent there for another email *policy* violation) and directly to the Outbound Queue.

- When there are two IronMail's in-line, **multiple actions** can be implemented. The Mail Monitoring Queue may be placed in the first position on IronMail-1 and re-route specific messages to another machine, while all the remaining messages are passed to IronMail-2 for regular examination.

Logging Quarantined MIME Parse Failures

IronMail offers the option of quarantining mime parse failures. The log for this action contains an entry that has an error code. Following is a partial list of the error codes and what they mean.

Error	Code	Description
RECURSION_LIMIT	101	There were too many MIME parts. (The maximum is 500.)
MKDIR_ERROR	102	Unable to create directories.
PFOPEN_ERROR	103	Unable to open files—probably because the files are not present.
MFOPEN_ERROR	104	Internal error.
MEMORY_ERROR	105	Internal memory error.
FOPEN_ERROR	106	Unable to open files—probably because the files are not present.
MIME_ERROR	107	Generic Invalid message based on type of format.
INVALID_UU_FORMAT	200	UUEncode is not in the correct format.

Only codes 101, 107, and 200 are shown on the log. The other codes are internal code used for troubleshooting.

Outbound Messages

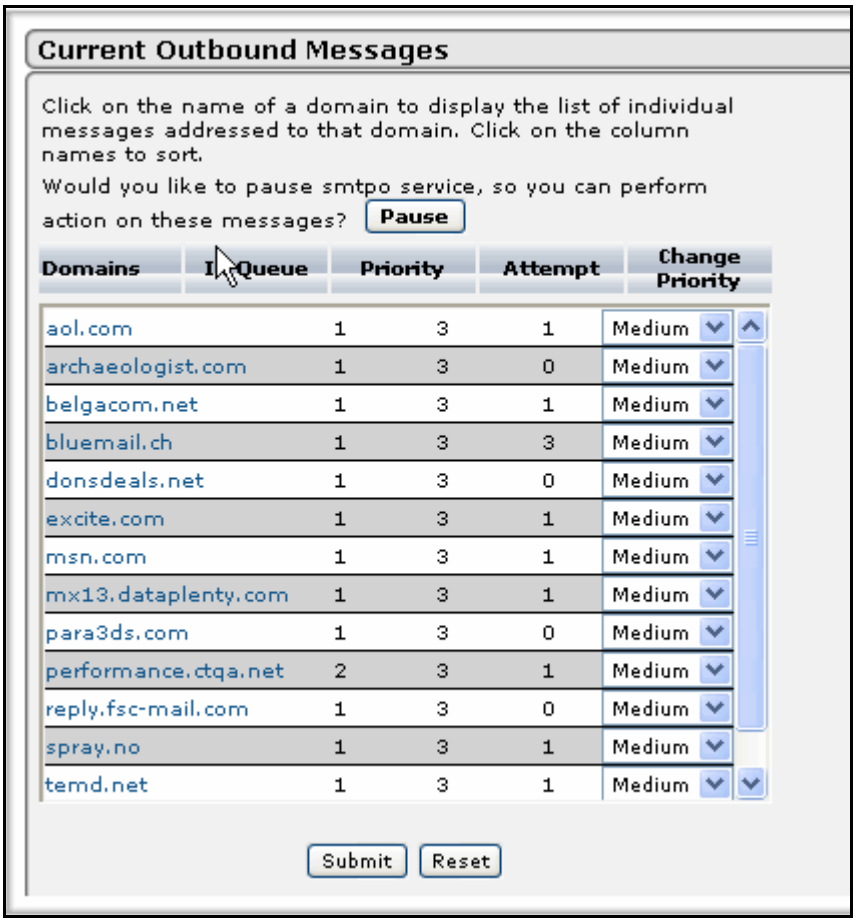
Outbound Queue

Just as IronMail offers visibility into the "inbound queues"—the processes that examine messages entering the appliance—it provides visibility and management of messages it is about to deliver off the appliance, both to internal users as well as to users out in the Internet.

The Outbound Queue hyperlink in the left navigation frame expands to offer Current Messages and Quarantined Messages sub-menus. The **Current Messages** hyperlink displays messages that have been examined by all the queues and are now waiting for the SMTPO Service to "pick them up" on its next cycle and deliver them. The **Quarantined Messages** hyperlink displays messages that were quarantined because the "Quarantine Undeliverable Messages" was enabled in the *Mail-Firewall > Configure Mail Services > SMTPO Services* properties page and IronMail could not successfully deliver them.

Current Messages

The Outbound Queue Current Messages table displays a list of all domains to whom one or more messages are addressed. (Note that the domains may be either external or internal—that is, messages addressed to users outside the *network*, or messages originating from outside the network and addressed to internal users.)

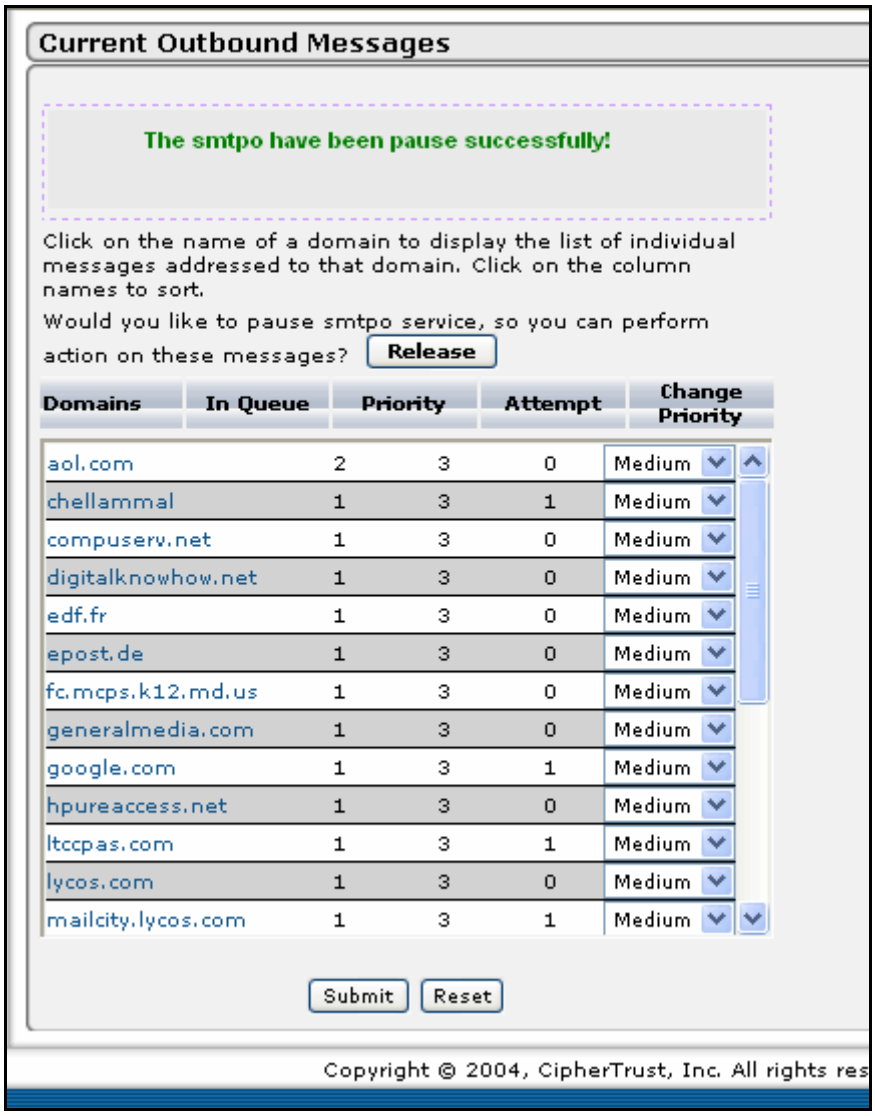

Current Outbound Messages
Click on the name of a domain to display the list of individual messages addressed to that domain. Click on the column names to sort.
Would you like to pause smtpo service, so you can perform action on these messages?
Pause
Domains
In Queue
Priority
Attempt
Change Priority
aol.com 1 3 1 Medium
archaeologist.com 1 3 0 Medium
belgacom.net 1 3 1 Medium
bluemail.ch 1 3 3 Medium
donsdeals.net 1 3 0 Medium
excite.com 1 3 1 Medium
msn.com 1 3 1 Medium
mx13.dataplenty.com 1 3 1 Medium
para3ds.com 1 3 0 Medium
performance.ctqa.net 2 3 1 Medium
reply.fsc-mail.com 1 3 0 Medium
spray.no 1 3 1 Medium
temd.net 1 3 1 Medium
Submit
Reset

The Outbound Queue Current Messages table displays the following information:

Domains	This column displays every domain to which one or more messages is addressed. The *domain name* is also a hyperlink that opens a Message Header window that displays information about each message addressed to that domain.
In Queue	This column displays the total number of messages, as of the moment the Outbound Queue Current Messages page was opened, are currently waiting to be delivered to the domain.
Priority	This column displays the priority of the domain. (IronMail assigns a default priority of "Medium" to every message as it arrives, unless a domain was manually assigned a different priority. IronMail will process "Highest" priority messages first, and "Least" priority messages last. The default priority for a domain can be changed in *Queue Manager > Domain Priority*.
Attempts	This column displays how many times IronMail has attempted to deliver a message. If a "Retry Schedule" was not entered in *Mail-Firewall > Configure Mail Services > SMTPO Service*, IronMail makes up to four additional attempts to deliver the message according to a default interval. If a retry schedule was provided, it makes up to four additional attempts to deliver the message according to the schedule. If the "Quarantine Undeliverable Messages" option was enabled in the SMTPO Service configuration, IronMail sends the message to the *Outbound Queue > Quarantined Messages Queue* after its fifth unsuccessful delivery attempt.

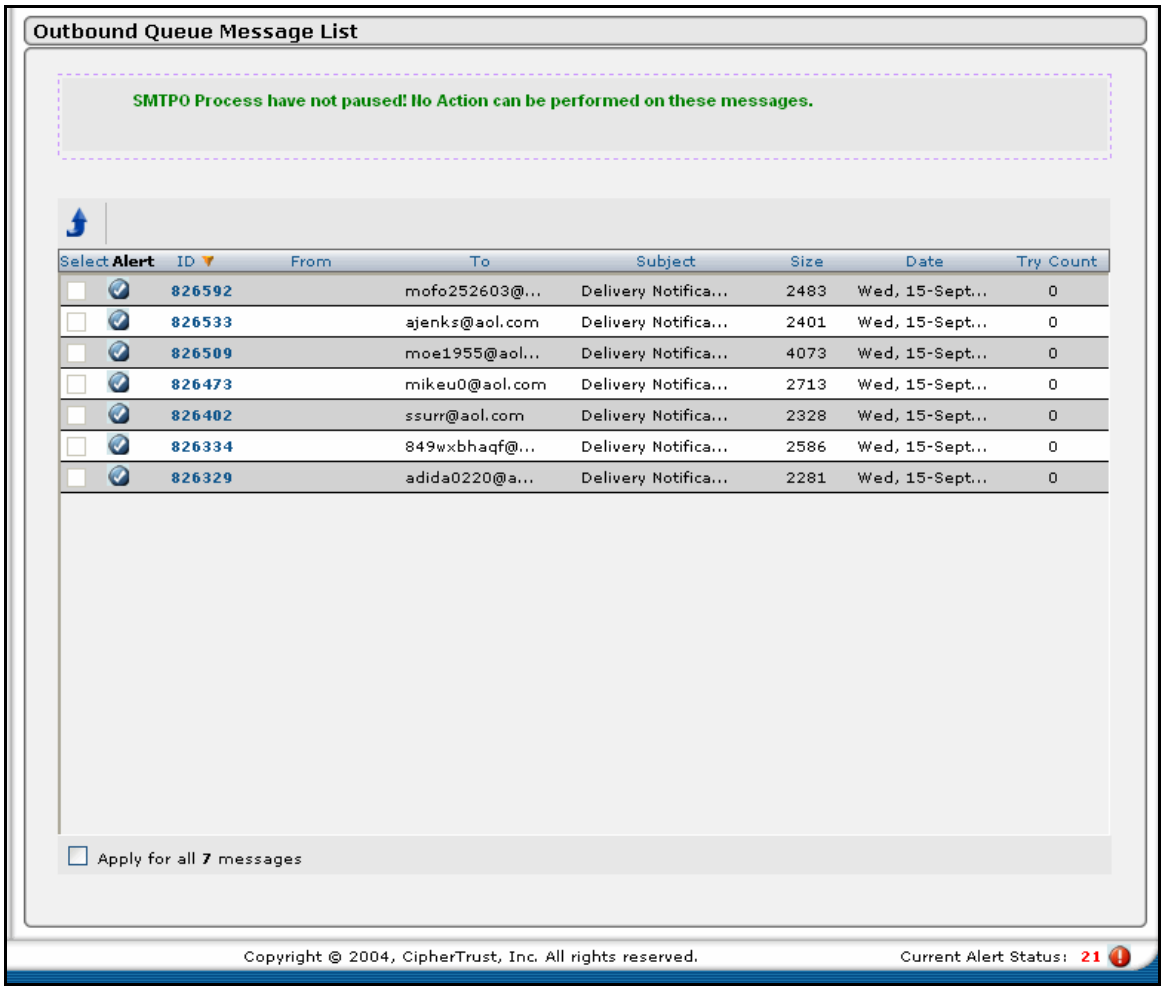
Change Priority	The **Change Priority** pick list lets the administrator temporarily change a domain's processing priority. The next time email to that domain enters the IronMail appliance, however, it is assigned the default priority of "Medium" again. (To make a priority persist, change its priority in *Queue Manager > Domain Priority*.)
Pause	The Pause button temporarily stops operation of the Outbound Queue to allow the Administrator to briefly review the messages contained there, and to take action on them.

When the Pause button is clicked, the Current Outbound Message window indicates a successful pause.


Current Outbound Messages
The smtpo have been pause successfully!
Click on the name of a domain to display the list of individual messages addressed to that domain. Click on the column names to sort.
Would you like to pause smtpo service, so you can perform action on these messages?
Release
Domains
In Queue
Priority
Attempt
Change Priority
aol.com 2 3 0 Medium
chellammal 1 3 1 Medium
compuserv.net 1 3 0 Medium
digitalknowhow.net 1 3 0 Medium
edf.fr 1 3 0 Medium
epost.de 1 3 0 Medium
fc.mcps.k12.md.us 1 3 0 Medium
generalmedia.com 1 3 0 Medium
google.com 1 3 1 Medium
hpureaccess.net 1 3 0 Medium
ltccpas.com 1 3 1 Medium
lycos.com 1 3 0 Medium
mailcity.lycos.com 1 3 1 Medium
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights res

IronMail's SMTPO Service, responsible for delivering messages out of the appliance, will stop all message delivery processing until the subsequent Outbound Message Header window is closed, or five minutes of inactivity elapse. Note that in a high mail volume environment (50,000+ messages per day), when the Outbound Queue is paused for even five minutes, messages will quickly backup, requiring intensive CPU processing in the following minutes in order to "catch up."

The Outbound Queue Message List window opens immediately after the Pause option is submitted.


Outbound Queue Message List
SMTPO Process have not paused! No Action can be performed on these messages.
Select Alert ID From To Subject Size Date Try Count
826592 mofo252603@... Delivery Notifica... 2483 Wed, 15-Sept... 0
826533 ajenks@aol.com Delivery Notifica... 2401 Wed, 15-Sept... 0
826509 moe1955@aol... Delivery Notifica... 4073 Wed, 15-Sept... 0
826473 mikeu0@aol.com Delivery Notifica... 2713 Wed, 15-Sept... 0
826402 ssurr@aol.com Delivery Notifica... 2328 Wed, 15-Sept... 0
826334 849wxbhaqf@... Delivery Notifica... 2586 Wed, 15-Sept... 0
826329 adida0220@a... Delivery Notifica... 2281 Wed, 15-Sept... 0
Apply for all 7 messages
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 21

The window, which allows the Administrator to take action, displays the following information:

Field	Description
Select	The checkbox is clicked to select one or more messages for action.
Alert	A checkmark icon in the list indicates that notification is to be sent when a message triggers a policy.
ID	This column displays a number that uniquely identifies the message. The ID number is a hyperlink that reveals details about the individual message.
From	This column displays the email address of the message sender.
To	This column displays the email address to whom the message is addressed.
Subject	This column displays the Subject line of the message. (Unlike the Message Header window for the incoming queues, this Subject line is not a hyperlink that opens a “management” window.)
Size	This column displays the size of the message.

Date	This column displays the date and timestamp when the SMTPO Service picked up the message for outbound delivery.
Try Count	If IronMail was unsuccessful delivering a message and a "Retry Schedule" was configured in *Mail-Firewall > Configure Mail Services > SMTPO Service*, the number of times IronMail has attempted to deliver the message is displayed in this column. (If a retry schedule was not configured, undeliverable messages are dropped, and this column will display "N/A.")

Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

To select all messages viewable within a domain's Message List window without scrolling through the window one page at a time, select **Apply For All nnn Messages** at the bottom of the secondary browser window. Note that while the secondary Message Header window is open, new messages may be entering the Outbound Queue addressed to that domain, even though message processing is temporarily paused. When this option is selected and an action is specified, the action does not affect the newly-received, but not yet viewed messages.

Clicking the Release button on the paused Outbound Messages window releases the Outbound Queue to continue its processing.

Quarantined Messages

The "Quarantine Undeliverable Messages" option for the SMTPO Service (*Mail-Firewall > Configure Mail Services*) instructs IronMail to send any message it is unable to deliver to the Outbound Queue's Quarantined Messages Queue. This queue provides administrative access to messages that haven't been delivered. The administrator may elect to delete the message, reschedule a future delivery attempt, or move the message back into the Outbound Queue for immediate delivery and another round of retry attempts.

Quarantined Outbound Messages
This table contains messages that could not be delivered, and were quarantined because the "Quarantine Undeliverable Messages" was enabled in Mail-Firewall > Configure Mail Services > SMTPO Service. Click a domain hyperlink to view the messages that were undeliverable. In the subsequent Message Header Detail window, select whether to delete the message or try delivering it again.
Domains
Quarantined Due To
Attempt
In Queue

The Outbound Queue's Quarantined Messages table displays the names of all domains to which undeliverable messages are addressed. The table displays the following information:

Domains	This column identifies the names of domains to which undeliverable messages are addressed. If messages to a domain were undeliverable for varying reasons, the domain will appear in this table multiple times—once for each type of error encountered. The *domain name* is also a hyperlink that opens a secondary browser window displaying all the individual messages addressed to that domain, and from which additional action may be taken.
Quarantined Due To	This column identifies the reason the message could not be delivered. The possible reasons are: • **TLS Failure:** IronMail could not deliver the message because TLS was required and an IronMail *policy* prohibited "falling back" to non-secure delivery. • **Domain same as IM:** If an email has a domain name identical to IronMail's *host name*, IronMail can get caught in a "loop," sending a message repeatedly to itself. IronMail will not allow this "looping" to happen. It will quarantine any message whose domain name is the same as IronMail's host name. • **Invalid Domain:** The domain name was typed incorrectly or the domain does not exist. • **Domain Unavailability:** The receiving server was unavailable. • **Recipient Refused:** The receiving server would not accept messages addressed to the recipient. Either the recipient's email address was

	mistyped, or the email account is no longer valid. • **Sender Refused:** The receiving mail server has a *rule* blocking messages from the sender. • **Data Error:** An error was encountered while transferring message data during the SMTP 821 transaction.
Attempts	This column displays how many times IronMail has attempted to deliver a message. If a "Retry Schedule" was not entered in *Mail-Firewall > Configure Mail Services > SMTPO Service*, IronMail makes up to four additional attempts to deliver the message according to a default interval. If a retry schedule was provided, it makes up to four additional attempts to deliver the message. If the "Quarantine Undeliverable Messages" option was enabled in the SMTPO Service configuration, IronMail sends the message to the *Outbound Queue > Quarantined Messages Queue* after its fifth unsuccessful delivery attempt.
In Queue	This column reports the numbers of messages, for each type of delivery error, addressed to each domain.

After clicking a domain name's hyperlink, a secondary Message List window opens, displaying all the individual messages addressed to that domain. Detailed information about the message is displayed. The Administrator may delete the message or "push" it to IronMail's SMTPO Service for immediately delivery.

Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

When the "**Apply For All *nnn* Messages**" check box at the bottom of the window displays a given number of messages, it is reporting the number of messages in that queue as of the moment the window was opened and that are viewable within this interface. To select all messages in the queue without scrolling through the window one page at a time, select **Apply For All *nnn* Messages** at the bottom of the window.

Note that the number in the **Try Count** column represents how many times in the current "retry cycle" the SMTPO Service has attempted to deliver a message. A zero value ("0") means that the SMTPO Service has exhausted all five delivery attempts. A value of four ("4") means that the SMTPO Service has made four delivery attempts and has one more attempt remaining. Bear in mind that each time the administrators clicks **Send Message(s) Now** for one or more messages, the retry cycle is reset. The administrator may indefinitely push messages to the Outbound Queue for repeated delivery attempts.

Searches

Searching for Messages within the Queue Manager

IronMail provides the ability to search for messages, whether *already delivered*, *still in the process of being delivered*, or currently sitting within its *quarantine queues*. Searching for messages can be useful when an administrator wants to determine if IronMail received a message for processing, whether it delivered it "off the box," and, if it is currently quarantined, to move it to the Outbound Queue for immediate delivery.

IronMail adds specific information to the RFC821 and RFC822 headers to facilitate quicker and more specific searches and better information gathering. The added information includes:

- the message ID - added to the RFC821 "received" information
- whitelist entry, if applicable - added to the RFC822 "from" header, in an X-header
- ESP score - added to the RFC822 "from" header, in an X-header

- applied policies - added to the RFC822 "from" header, in an X-header
- actions taken - added to the RFC822 "from" header, in an X-header

Note: Much of the RFC822 data shown above is included in a single X-header containing information about the message from IronMail's logs.

As an example of ways this information will help, assume a user sends a message back to the Administrator, saying the message should have been caught as spam. If the message ID is in the header, the Administrator can find it easily and quickly search for the message in the Processed Messages area, and thereby determine what actions to take.

Partial information may be entered in IronMail's search input fields. (A search for "dscott" will find dscott@domain.com). If search values are entered in more than one input field, IronMail will not find the message unless the values are found in all used fields.

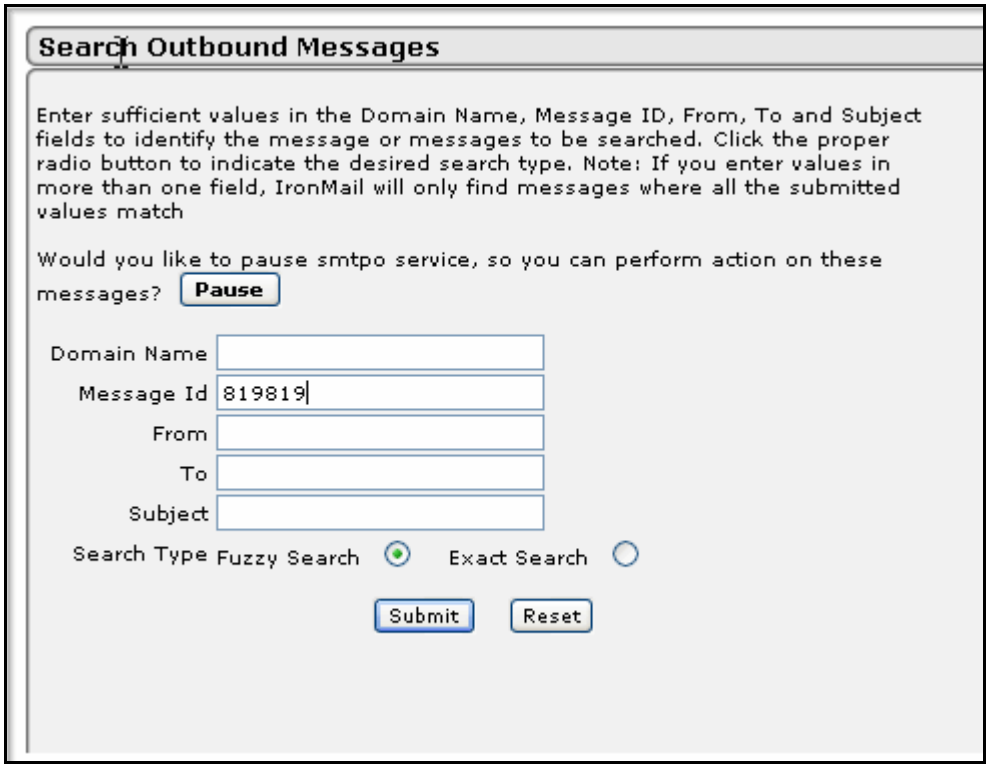
The results of the search are displayed in a Search Results window in the main body of the page. If more than one message matching the search criteria is found, they appear in separate rows of the Search Results table. Clicking a message's **Subject** hyperlink within the table opens a secondary window from which various administrative actions may be taken, depending on whether or not the message is still on the IronMail appliance.

The **Search** hyperlink in the left navigation frame under Queue Manager expands to reveal Current Messages, Quarantined Messages, and Processed Messages sub-menus. The **Current Messages** hyperlink allows administrators to search for messages currently being processed by IronMail's queues. The **Quarantined Messages** hyperlink allows administrators to search for messages inside one of IronMail's quarantine queues. The **Processed Messages** hyperlink allows administrators to search for messages that have already been delivered. The user interface for searching within each of these pages is nearly identical.

Current Messages

The Current Messages Search window offers varying input fields for entering search criteria, depending on where the administrator is searching for current outbound messages or current messages in queues.

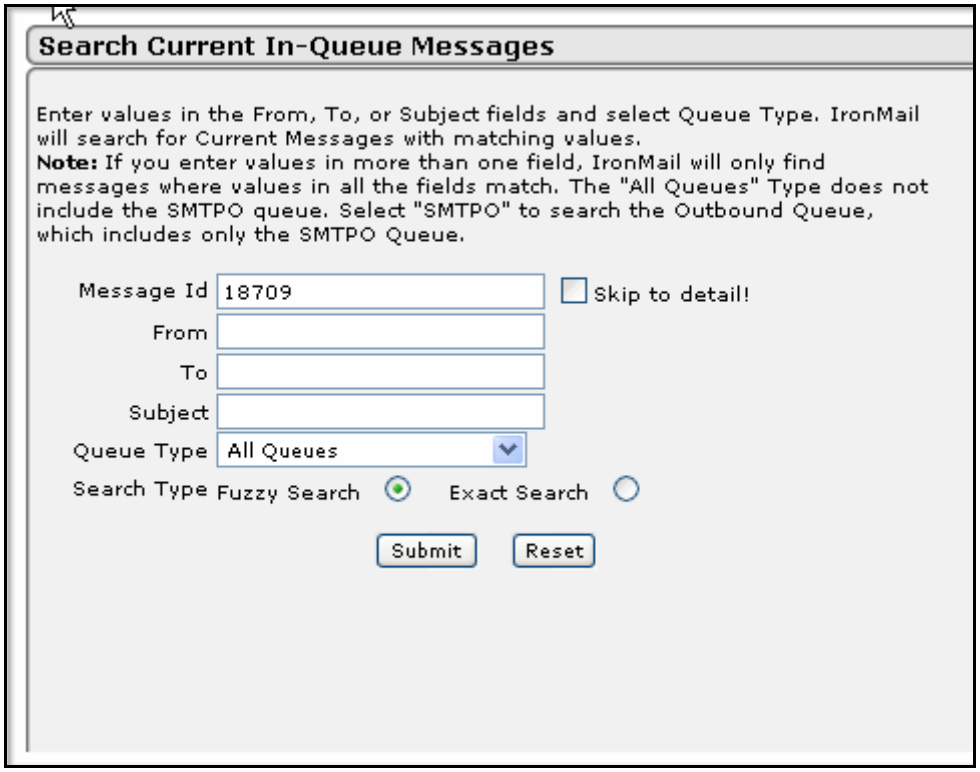
The Search Outbound Messages window offers a Pause button to allow the Administrator to temporarily pause the Outbound Queue and view the messages there.


Search Outbound Messages
Enter sufficient values in the Domain Name, Message ID, From, To and Subject fields to identify the message or messages to be searched. Click the proper radio button to indicate the desired search type. Note: If you enter values in more than one field, IronMail will only find messages where all the submitted values match
Would you like to pause smtpo service, so you can perform action on these messages?
Pause
Domain Name
Message Id
819819
From
To
Subject
Search Type
Fuzzy Search
Exact Search
Submit
Reset

The screen offers the following fields for search parameters:

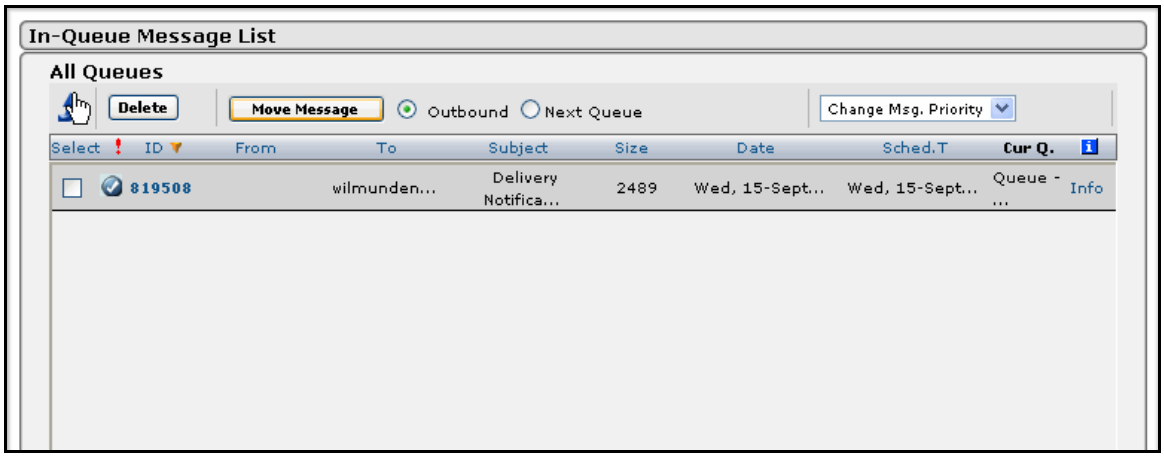
Field	Description
Domain Name	Enter the domain name for the destination domain to which the message is being sent.
Message ID	Enter the message ID for the specific message.
From	Enter the RFC822 From address in the input field.
To	Enter the RFC822 To address in the input field.
Subject	Enter the Subject line in the input field.
Search Type	Select the radio button to indicate the type of search IronMail is to conduct: • Fuzzy Search • Exact Search

The Search Current In-Queue Messages screen displays as follows:


Search Current In-Queue Messages
Enter values in the From, To, or Subject fields and select Queue Type. IronMail will search for Current Messages with matching values.
Note: If you enter values in more than one field, IronMail will only find messages where values in all the fields match. The "All Queues" Type does not include the SMTPO queue. Select "SMTPO" to search the Outbound Queue, which includes only the SMTPO Queue.
Message Id
18709
Skip to detail!
From
To
Subject
Queue Type
All Queues
Search Type
Fuzzy Search
Exact Search
Submit
Reset

Field	Description
Message ID	Enter the message ID for the particular message.
From	Enter the RFC822 From address in the input field.
To	Enter the RFC822 To address in the input field.
Subject	Enter the Subject line in the input field.
Queue Type	From the drop-down list, select the type of queue to be searched for the message. Options are: • All Queues • Super Queue • Virus Scan • Content Filtering • Mail Monitoring • Anti-Spam
Search Type	Select the radio button to indicate the type of search IronMail is to conduct: • Fuzzy Search • Exact Search

Click the **Submit** button below the search criteria input fields. A Search Results page loads in the main content frame of the Web Administration interface, showing all messages that matched the search criteria.



In addition to showing the results of a search, the search results page provides administrators with the ability to take action from a list of messages located through the search function. For example, administrators may delete messages and move them to the Outbound Queue. (Messages that the queue has already begun to process are not displayed in the secondary window and cannot be deleted or otherwise "managed.")

The search results (Message List) window displays up to 20 messages at a time. If more than twenty messages are currently in the queue, a **"Next"** hyperlink is displayed at the ***top*** of the Message Header table, allowing navigation to the next twenty messages. After navigating "forward" through one of more pages of messages, a **"Previous"** hyperlink is displayed, allowing backward navigation through the contents of the queue. Note that the messages visible in the Message List table are statically displayed—messages that enter the queue *while the search results table is open* are not displayed until the Message List window is closed and reopened again. When the "**Apply For All *nnn* Messages**" check box at the bottom of the Message List window displays a given number of messages, it is reporting the number of messages in that queue as of the moment the Message Header window was opened and that are viewable within this interface. To select all messages viewable within the Search Results window without having to scroll through the window one page at a time, select "**Apply For All nnn Messages.**"

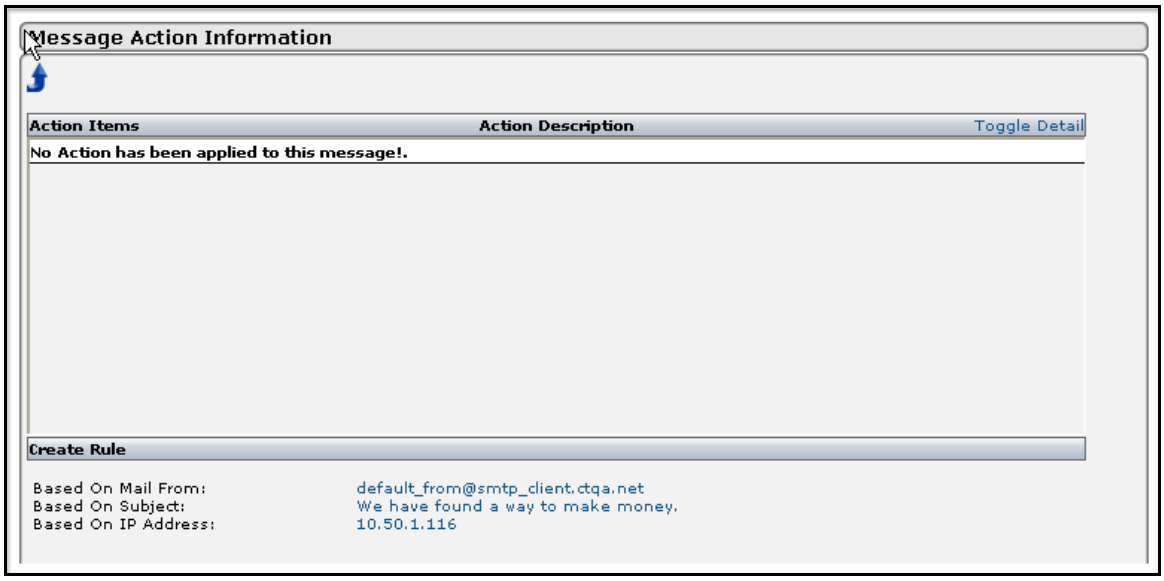
When the Message List window opens, that queue pauses all processing until the window is closed or five minutes of inactivity elapse. Note, however, that IronMail's Auto Refresh function will *release* paused queues on the refresh schedule, even if the five minutes of inactivity have not yet transpired. Administrators should be aware, therefore, that if they expect to perform email management within a queue, a short Auto Refresh rate may impact their ability to process those messages.

The Message List table displays the following information:

Field	Description
Delete	The **Delete** button deletes all selected messages, whether selected individually, by clicking the Select column heading hyperlink, or selecting the **Apply For All Messages** check box. Deleted messages are not delivered, and are removed from IronMail's database. (IronMail's SMTPO log file will report that the messages were deleted.)
Move Message	The Administrator can choose to move one or more messages out ot the current queue. Options are: • **Outbound** - moves all selected messages to IronMail's SMTPO Outbound Queue. They bypass any remaining queues that have not yet processed the messages.

	• **Next Queue** - moves selected message (one at a time) to the next queue in line for processing.
Change Message Priority	The **Change Priority** pick list lets the administrator temporarily change a domain's processing priority. The next time email to that domain enters the IronMail appliance, however, it is assigned the default priority of "Medium" again. (To make a priority persist, change its priority in *Queue Manager > Domain Priority*.)
Select	A **Select** check box allows administrators to select one or more messages for administrative action. Clicking the **Select** column heading hyperlink selects all messages on the page. IronMail remembers messages that have been selected when administrators navigate through multiple pages. For example, if a message is selected on the first "page" of the Search Results window for the purpose of deleting it, and the administrator navigates two pages forward to select another message, both messages will be deleted when clicking the **Delete Message(s)** button at the bottom of the window. Alternately, the administrator may repeatedly click the **Select** column heading hyperlink on each page to select all messages on multiple pages for deletion or for movement to the Outbound Queue. To select all messages viewable within the Search Results window without scrolling through the window one page at a time, select "**Apply For All nnn Messages**" at the bottom of the secondary browser window. Note that while the secondary Search Messages window is open, new messages may be entering the queue, even though message processing is temporarily paused. When this option is selected and an action is specified, the action does not apply to the newly-received, but not yet displayed messages.
ID	This column displays a number that uniquely identifies the message. The ID is also a hyperlink that reveals message details.
From	This column displays the RFC822 From address of the message sender. The From column heading is a hyperlink that sorts the Message Header table by From address in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened again.
To	This column displays the RFC822 To address of the message sender. The To column heading is a hyperlink that sorts the Message Header table by To address in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Message Header window is closed and reopened.
Subject	This column displays the message's Subject Line. The Subject line is also a hyperlink that opens a tertiary Message Detail window displaying a variety of administrative actions that can be taken for the message. (See below.) Whereas only two actions are possible when selecting multiple messages (**Delete** and **Move to the Outbound Queue**), additional actions may be available through the tertiary window's interface when clicking the Subject of a single message: • The message priority may be changed. • The message may be moved to any other queue remaining to process it. • The message may be given a manually-assigned delivery date. • The message may be forwarded to an alternate email address. • The message header, body, and attachments may be viewed.
Size	This column indicates the size of the message in kilobytes.
Date	This field shows the date the message was received.

Sched. T	The date in this field represents the time when the message will be pushed on to the next queue or deleted.
Current Queue	This column displays the IronMail queue where the message is currently being processed. All the Queues are paused for search process.
Info	Clicking the Info hyperlink for any messages displays action information for that message.



Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

Warning: To prevent inadvertent delivery of infected messages, do not attempt to move virus infected messages to the Outbound queue.

Quarantined Messages

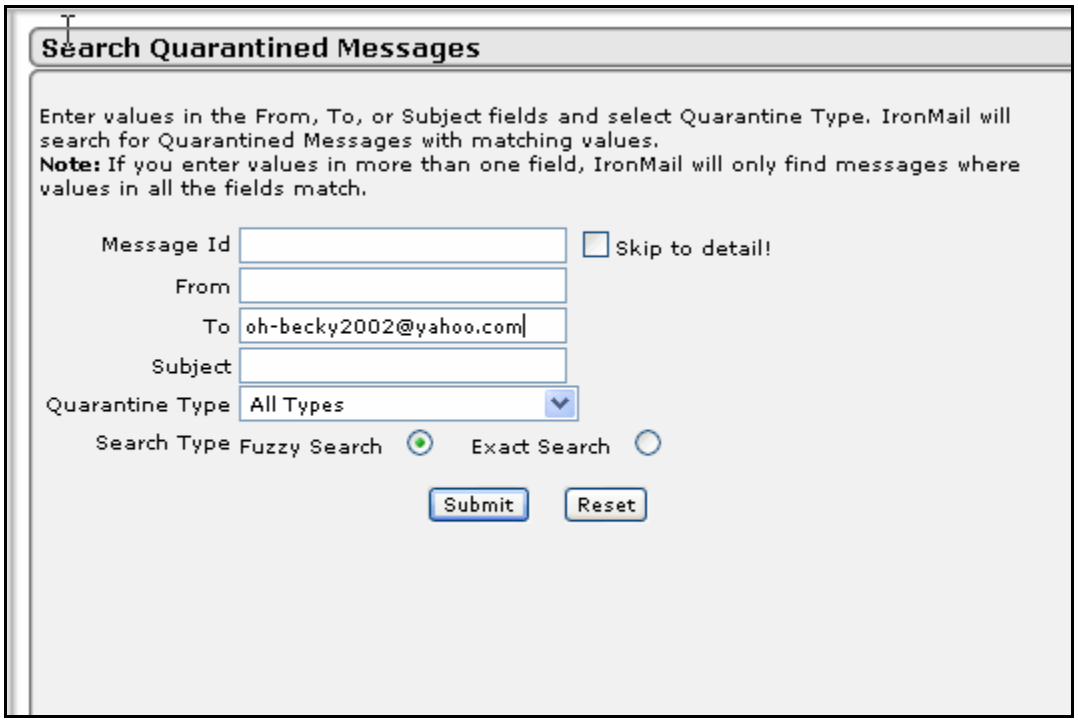
The Message Search window offers varying input fields for entering search criteria, depending on where the administrator is searching for messages: quarantined outbound messages, or quarantined messages in queues.

Search Quarantined Outbound Messages
Enter sufficient values in the Domain Name, Message ID, From, To and Subject fields to identify the message or messages to be searched. Click the proper radio button to indicate the desired search type. Note: If you enter values in more than one field, IronMail will only find messages where all the submitted values match
Domain Name
Message Id
From
To
user@performance.ctqa.net
Subject
Search Type
Fuzzy Search
Exact Search
Submit
Reset

The search window for Quarantined Outbound Queues offers the following options:

Field	Description
Domain Name	Enter the domain name for the message.
Message ID	Enter the message ID for the specific message.
From	Enter the RFC822 From address in the input field.
To	Enter the RFC822 To address in the input field.
Subject	Enter the Subject line in the input field.
Search Type	Select the radio button to indicate the type of search IronMail is to conduct: • Fuzzy Search • Exact Search

Enter the desired parameters in the Search Quarantined Messages window to find messages currently in queues.


Search Quarantined Messages
Enter values in the From, To, or Subject fields and select Quarantine Type. IronMail will search for Quarantined Messages with matching values.
Note: If you enter values in more than one field, IronMail will only find messages where values in all the fields match.
Message Id
Skip to detail!
From
To
oh-becky2002@yahoo.com
Subject
Quarantine Type
All Types
Search Type
Fuzzy Search
Exact Search
Submit
Reset

Field	Description
Message ID	Enter the domain name for the message.
From	Enter the RFC822 From address in the input field.
To	Enter the RFC822 To address in the input field.
Subject	Enter the Subject line in the input field.
Quarantine Type	From the drop-down list, select the quarantine/queue type associated with the message. Options are: • All Types • Anti-Spam • Anti-Virus • Attachment Filtering • Content Filtering • Encrypted Message • Failures • Mail Monitoring • Off-Hour • SMTPO
Search Type	Select the radio button to indicate the type of search IronMail is to conduct: • Fuzzy Search • Exact Search

Click the **Submit** button below the search criteria input fields. A Search Results page loads in the main content frame of the Web Administration interface, showing all messages that matched the

search criteria. IronMail queue services (such as the Content Filtering Queue and the Mail Monitoring Queue) continue to process messages during the Quarantined Messages Queue search. The Search Results table displays the following information:

In addition to showing the results of a search, the Quarantined Messages page provides administrators with the ability to take action from a list of messages located through the search function. For example, administrators may delete messages and move them to the Outbound Queue. (Messages that the queue has already begun to process are not displayed in the secondary window and cannot be deleted or otherwise "managed.") The Message Header window is also useful for obtaining a Message ID before investigating messages listed in the Anti-Spam Queue Detailed Log.

The Quarantined Messages window displays up to 20 messages at a time. If more than twenty messages are currently in the queue, a **"Next"** hyperlink is displayed at the top of the Message Header table, allowing navigation to the next twenty messages. After navigating "forward" through one of more pages of messages, a **"Previous"** hyperlink is displayed, allowing backward navigation through the contents of the queue. Note that the messages visible in the Quarantined Messages window are statically displayed—messages that enter the queue *while the Quarantined Messages window is open* are not displayed until the Quarantined Messages window is closed and reopened again. When the "**Apply For All *nnn* Messages**" check box at the bottom of the Message Header window displays a given number of messages, it is reporting the number of messages in that queue as of the moment the Message Header window was opened and that are viewable within this interface. To select all messages viewable within the Search Results window without having to scroll through the window one page at a time, select "**Apply For All nnn Messages.**"

When the Quarantined Messages window opens, that queue pauses all processing until the window is closed or five minutes of inactivity elapse. Note, however, that IronMail's Auto Refresh function will *release* paused queues on the refresh schedule, even if the five minutes of inactivity have not yet transpired. Administrators should be aware, therefore, that if they expect to perform email management within a queue, a short Auto Refresh rate may impact their ability to process those messages.

The Quarantined Messages window displays the following information:

Field	Description
Select	A **Select** check box allows administrators to select one or more messages for administrative action. Clicking the **Select** column heading hyperlink selects all messages on the page. IronMail remembers messages that have been selected when administrators navigate through multiple pages. For example, if a message is selected on the first "page" of the Message Header window for the purpose of deleting it, and the administrator navigates two pages forward to select another message, both messages will be deleted when clicking the **Delete Message(s)** button at the bottom of the window. Alternately, the administrator may repeatedly click the **Select** column heading hyperlink on each page to select all messages on multiple pages for deletion or for movement to the Outbound Queue. To select all messages viewable within the Message Header window without scrolling through the window one page at a time, select "**Apply For All nnn Messages**" at the bottom of the secondary browser window. Note that while the secondary Message Header window is open, new messages may be entering the queue, even though message processing is temporarily paused. When this option is selected and an action is specified, the action does not apply to the newly-received, but not yet displayed messages.

ID	This column displays a number that uniquely identifies the message. This number is the Message ID used to troubleshoot messages handling using the Anti-Spam Queue Detailed Log.
From	This column displays the RFC822 From address of the message sender. The From column heading is a hyperlink that sorts the Quarantined Messages table by From address in ascending and descending order. When the Quarantined Messages table is sorted, IronMail preserves the sort until a new sort is applied or until the window is closed and reopened again.
To	This column displays the RFC822 To address of the message sender. The To column heading is a hyperlink that sorts the Quarantined Messages table for the purpose of deleting it, and the administrator table by To address in ascending and descending order. When the Message Header table is sorted, IronMail preserves the sort until a new sort is applied or until the Quarantined Messages window is closed and reopened.
Subject	This column displays the message's Subject Line.
Size	The column shows the size, in kilobytes, of each message.
Date	This field shows the date the message is received.
Sched. T	This column lists the date when the message is scheduled to be pushed to the next queue for processing, or deleted.
Current Queue	The field contains the name of the current queue where the message is presently stored.
Info	Clicking the Info hyperlink opens a window that displays message detail.

Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

At the bottom of the Search Results window are three buttons.

Delete Message(s)	The **Delete** button deletes all selected messages, whether selected individually, by clicking the Select column heading hyperlink, or selecting the **Apply For All Messages** check box. Deleted messages are not delivered, and are removed from IronMail's database. (IronMail's SMTPO log file will report that the messages were deleted.)
Move to Outbound Queue	The **Move to Outbound Queue** button moves all selected messages to IronMail's SMTPO Outbound Queue. They bypass any remaining queues that have not yet processed the messages. Note that multiple messages cannot be moved in a batch to the next queue in-line to process them. Pushing messages to the next queue in-line must be done one message at a time.
Release	The **Release** button releases the "pause" action for the queue—it immediately resumes processing messages within it. (IronMail automatically stops a queue from processing messages when an administrator opens a queue's Message Header Detail window. The queue remains paused as long as the window is open or five minutes of inactivity lapse.)

Whenever a message's **Subject** hyperlink is clicked within a Quarantined Messages window, a secondary Message Detail window opens, displaying:

Delete Message(s)	The **Delete** button deletes all selected messages, whether selected individually, by clicking the Select column heading hyperlink, or selecting the **Apply For All Messages** check box. Deleted messages are not delivered, and are removed from IronMail's database. (IronMail's SMTPO log file will report that the messages were deleted.)
Move to Outbound Queue	The **Move to Outbound Queue** button moves all selected messages to IronMail's SMTPO Outbound Queue. They bypass any remaining queues that have not yet processed the messages. Note that multiple messages cannot be moved in a batch to the next queue in-line to process them. Pushing messages to the next queue in-line must be done one message at a time.
Action	The **Action** button opens a tertiary window in which various actions are possible, depending on which queue the message is in, and how many queues remain to process the message: • The message priority may be changed. • If only one message is selected, the message may be moved to any other queue remaining to process it. • If the message is currently in a quarantine queue, the delivery date may be rescheduled. • If the message is currently in a quarantine queue, the message may be forwarded to an alternate email address. Note that the administrator may not "push" multiple messages to the *next queue in line*. Messages in the Quarantine Queue may be there because different queue subsystems enforced their own email policies on them. IronMail is not able to perform a batch process that checks, for each message, which queue has already processed it and which ones remain. When multiple messages are selected and the administrator wants to "push" them forward, he or she must move them directly to the Outbound Queue by clicking Move to Outbound Queue.
Close	The **Close** button closes the Message Header window without performing any actions. When the Message Header Window is closed, IronMail releases the "pause" action for the queue—it immediately resumes processing messages within it.

Note: Messages that have a Virus icon in the same row were found to contain viruses. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

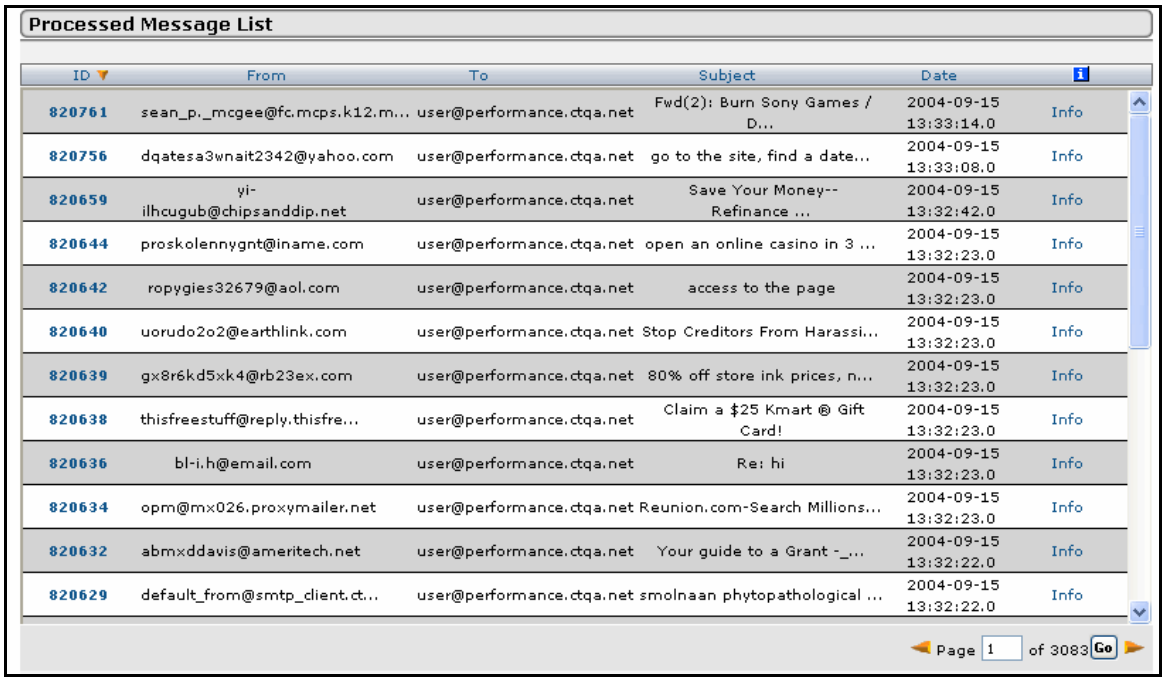
Processed Messages

The Message Search window offers four fields for entering search criteria for messages that have already been processed but which have not yet been delivered.

Field	Description
Message ID	Enter the message ID for the message.
Skip to Detail	If the message ID is entered, clicking the check box will open the message details for that specific message when you click **Submit**.
From	Enter the RFC822 From address in the input field.
To	Enter the RFC822 To address in the input field.
Subject	Enter the Subject line in the input field.
Search Type	Select the radio button to indicate the type of search IronMail is to conduct: • Fuzzy Search • Exact Search

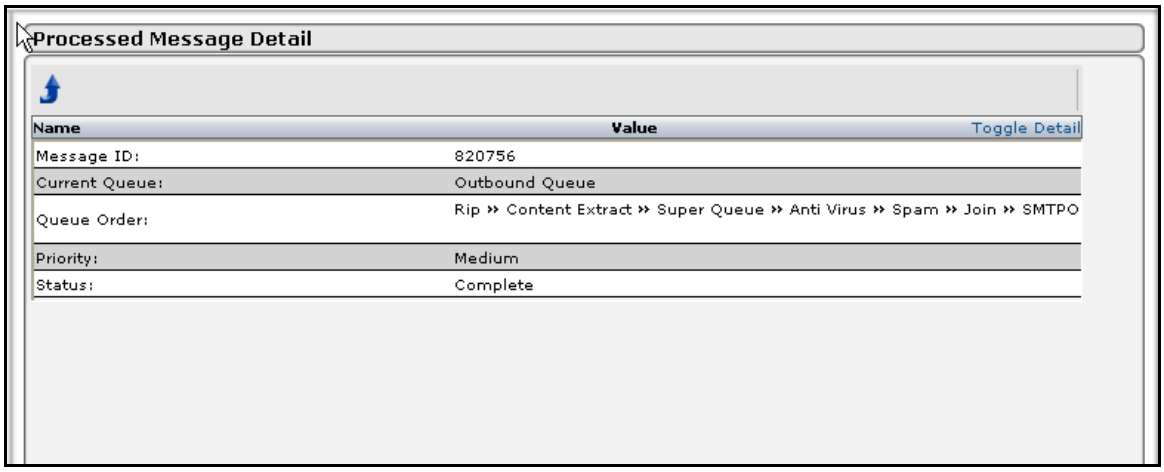
Click the **Submit** button below the search criteria input fields. A search results page loads in the main content frame of the Web Administration interface, showing all messages that matched the search criteria. IronMail queue features (such as Content Filtering and Mail Monitoring) continue to process messages during the Processed Messages Queue search. The search results window is also useful for obtaining the Message ID before investigating messages listed in the Anti-Spam Queue Detailed Log.

The Processed Message List displays the following information:

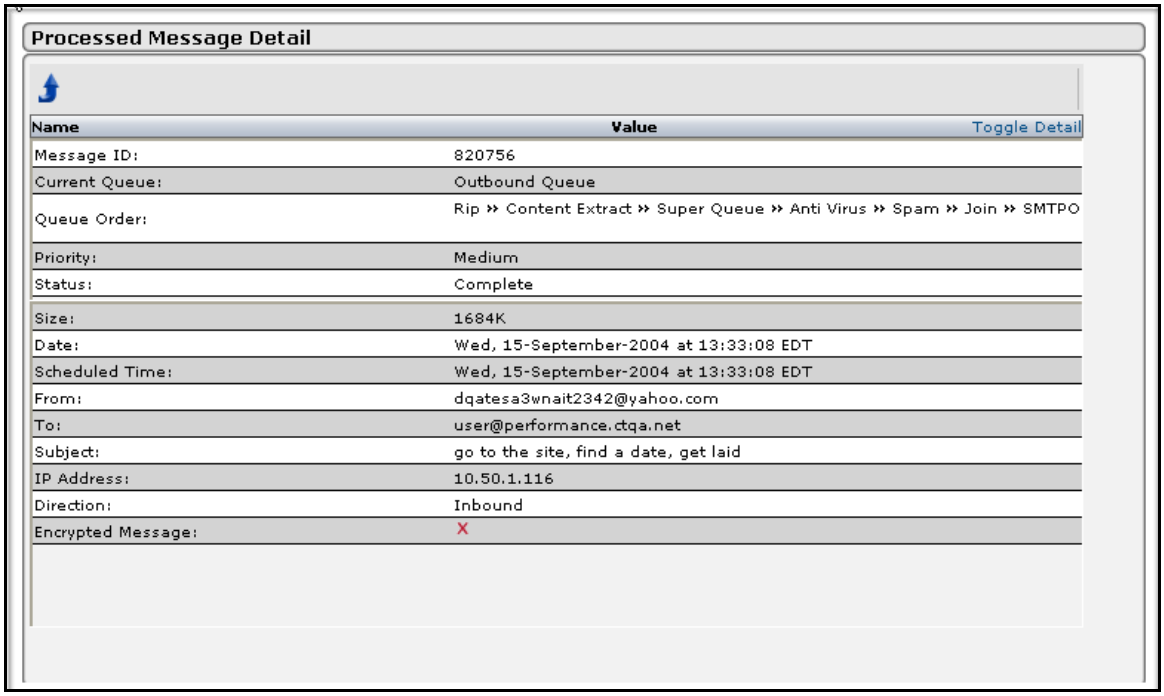

Processed Message List
ID
From
To
Subject
Date
820761 sean_p._mcgee@fc.mcps.k12.m... user@performance.ctqa.net Fwd(2): Burn Sony Games / D... 2004-09-15 13:33:14.0 Info
820756 dqatesa3wnait2342@yahoo.com user@performance.ctqa.net go to the site, find a date... 2004-09-15 13:33:08.0 Info
820659 yi-ilhcugub@chipsanddip.net user@performance.ctqa.net Save Your Money--Refinance ... 2004-09-15 13:32:42.0 Info
820644 proskolennygnt@iname.com user@performance.ctqa.net open an online casino in 3 ... 2004-09-15 13:32:23.0 Info
820642 ropygies32679@aol.com user@performance.ctqa.net access to the page 2004-09-15 13:32:23.0 Info
820640 uorudo2o2@earthlink.com user@performance.ctqa.net Stop Creditors From Harassi... 2004-09-15 13:32:23.0 Info
820639 gx8r6kd5xk4@rb23ex.com user@performance.ctqa.net 80% off store ink prices, n... 2004-09-15 13:32:23.0 Info
820638 thisfreestuff@reply.thisfre... user@performance.ctqa.net Claim a $25 Kmart ® Gift Card! 2004-09-15 13:32:23.0 Info
820636 bl-i.h@email.com user@performance.ctqa.net Re: hi 2004-09-15 13:32:23.0 Info
820634 opm@mx026.proxymailer.net user@performance.ctqa.net Reunion.com-Search Millions... 2004-09-15 13:32:23.0 Info
820632 abmxddavis@ameritech.net user@performance.ctqa.net Your guide to a Grant -_... 2004-09-15 13:32:22.0 Info
820629 default_from@smtp_client.ct... user@performance.ctqa.net smolnaan phytopathological ... 2004-09-15 13:32:22.0 Info
Page 1 of 3083 Go

Field	Description
ID	This column displays a number that uniquely identifies the message. This number is the Message ID used to troubleshoot messages listed in the Anti-Spam Queue Detailed Log. The ID is also a hyperlink that reveals message details.
From	This column displays the messages' From address. This column displays the RFC822 From address of the message sender. The From column heading is a hyperlink that sorts the Search Results table by From address in ascending and descending order. When the Search Results table is sorted, IronMail preserves the sort until a new sort is applied or until the window is closed and reopened again.
To	This column displays the messages' To address. The To column heading is a hyperlink that sorts the Search Results table for the purpose of deleting it, and the administrator table by To address in ascending and descending order. When the Search Results table is sorted, IronMail preserves the sort until a new sort is applied or until the Search Results window is closed and reopened.
Subject	This column displays the messages' Subject line. The Subject line is also a hyperlink that opens a secondary Message Detail window in which administrative tasks may be performed, depending on whether or not the message has been delivered.
Date	This column shows the date and time the message was processed.
Info	Clicking the Info hyperlink displays action information about the specific message.

Clicking the Info hyperlink for a message opens the Processed Message Detail screen.



You may view the message information in its abbreviated form, as above, or click the Toggle Data hyperlink to expand the available information.

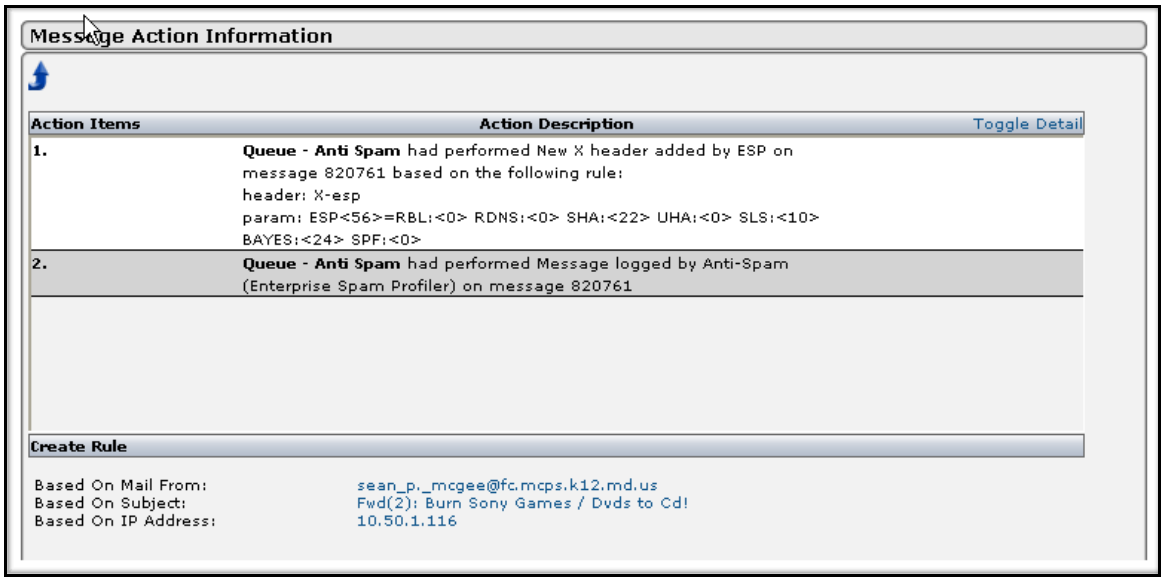


The following information can be viewed in two columns containing the field name and the associated value for that field.

Field	Description
Message ID	The unique message ID number can be used to track the message using the logs and reports.
Current Queue	This is the current location (queue name) where the message is stored.
Queue Order	This field reveals the order in which IronMail's queues and features processed the message.
Priority	The assigned priority displays in this field.
Status	The current status of the message appears here (e.g., Complete).

Size	This field shows the size of the message in kilobytes.
Date	The system date and time when the message was processed displays in this field.
Scheduled Time	This field shows the date and time when the message should be delivered.
From	This is the From address for the message.
To	This is the recipient address.
Subject	This field shows the subject line from the processed message.
IP Address	This field displays the IP address to which the message will be delivered.
Direction	This is the message direction: inbound or outbound.
Encrypted Message	If this is an encrypted message, an "X" will appear in this field.

Clicking the Info hyperlink on the Processed Message List screen displays details about actions taken on the message in question.


Message Action Information
Action Items
Action Description
Toggle Detail
1.
Queue - Anti Spam had performed New X header added by ESP on message 820761 based on the following rule:
header: X-esp
param: ESP<56>=RBL:<0> RDNS:<0> SHA:<22> UHA:<0> SLS:<10> BAYES:<24> SPF:<0>
2.
Queue - Anti Spam had performed Message logged by Anti-Spam (Enterprise Spam Profiler) on message 820761
Create Rule
Based On Mail From:
sean_p._mcgee@fc.mcps.k12.md.us
Based On Subject:
Fwd(2): Burn Sony Games / Dvds to Cd!
Based On IP Address:
10.50.1.116

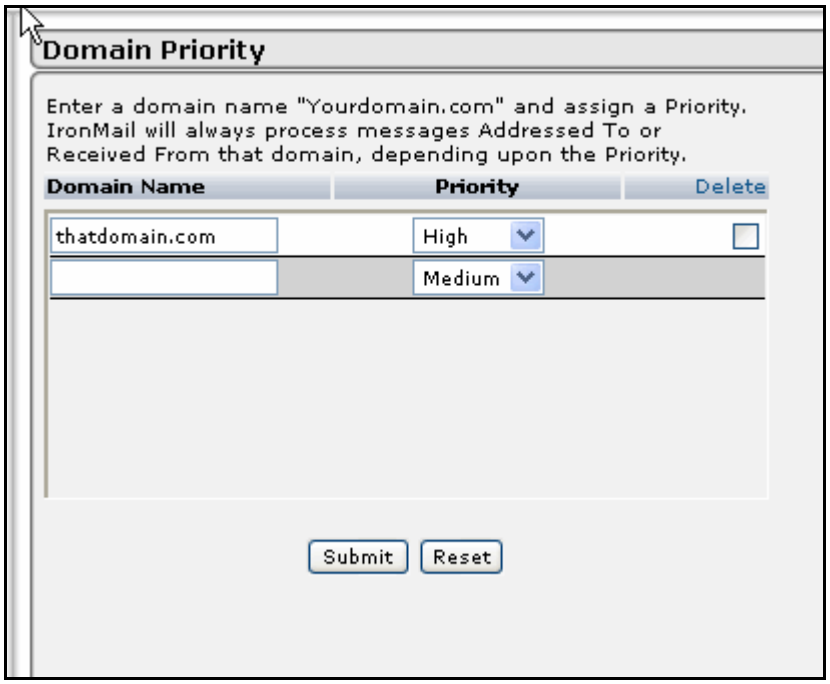
User Tip

Many administrators will use IronMail for spam-blocking. Though IronMail can achieve a very low rate of false positives, some administrators feel more comfortable setting the spam tools' action to "Quarantine" instead of "Drop," and set the quarantine value to zero so IronMail's Cleanup Schedule deletes the messages after *nnn* number of days. When individuals report that email they are expecting has not yet arrived, administrators can search for the message in the Quarantine Queue, and if present, move it to the Outbound Queue for immediately delivery.

Domain Priority

IronMail orders the processing of all messages within its queues on the basis of a message's "priority." By default, IronMail assigns each message entering the appliance a priority of "Medium." (The Rip Queue, the first to process messages after they have been received by IronMail's SMTPI Service, "picks up" a given number of messages at a time for ripping into their separate *MIME* parts. Each subsequent queue picks up "batches" of messages and processes them. Within each "batch" or group of messages picked up for processing, IronMail processes messages with a "Highest" priority first, and "Least" priority last. If messages from more than one domain each have the same priority—e.g., "Highest"—the messages are processed ahead of the

others, but in the order in which they entered the IronMail appliance.) To ensure that email from certain domains is always processed before others,' assign the domain a persistent priority. When messages from those domains enter IronMail, the SMTPI Service looks in the Domain Priorities table and (internally) stamps the message with the specified priority. As the message traverses each queue, it is processed earlier or later than the others.



Administrators typically add the names of their own domains, and the domains of their business partners in this page, and assign them the "Highest" priority.

The Domain Priority page, empty until one or more domains have been added, allows the following user input:

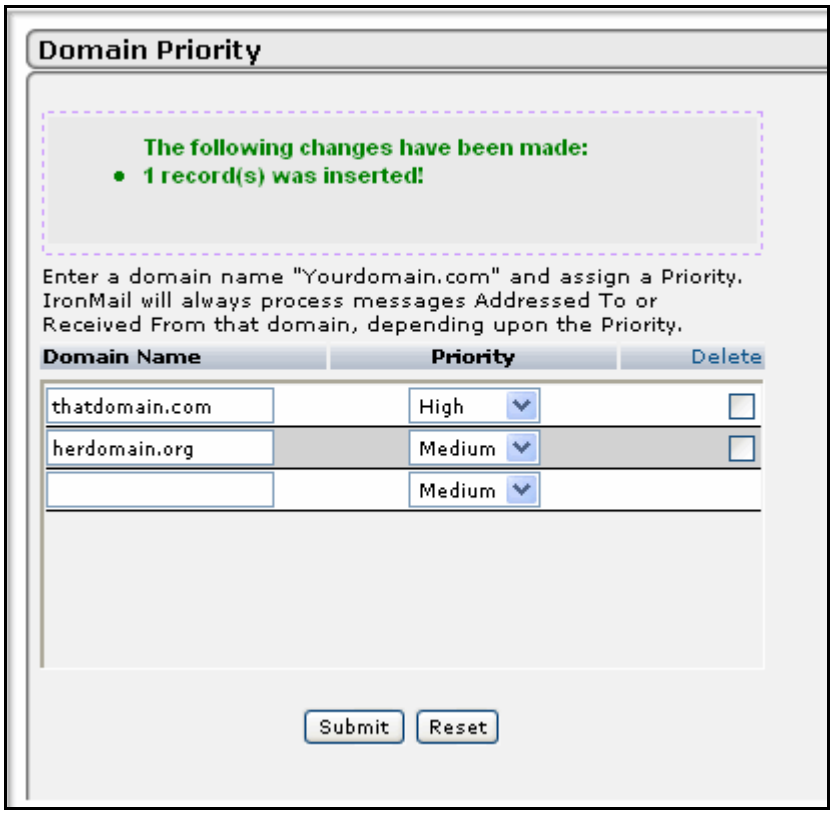
Field	Description
Domain Name	This field shows the domain name for each domain that has been added and for which priority has been set.
Priority	The selected priority displays here. Options are: • Highest • High • Medium • Low • Lowest
Delete	To remove a domain from the Domain Priority table, select its **Delete** check box and click **Submit**.

Adding or Editing a Domain

You can add a domain from the Domain Priority window.

Field	Description
Domain Name	Enter a valid domain name in the **Domain name** input field, e.g., mydomain.com.
Priority	Select a priority from the pick list beside it. Options are: • Highest • High • Medium • Low • Lowest You may change the priority of an existing domain by selecting a new one and clicking **Submit**.
Delete	To remove a domain from the Domain Priority table, select its **Delete** check box and click **Submit**.

When changes are submitted, the window will display the new priority list.

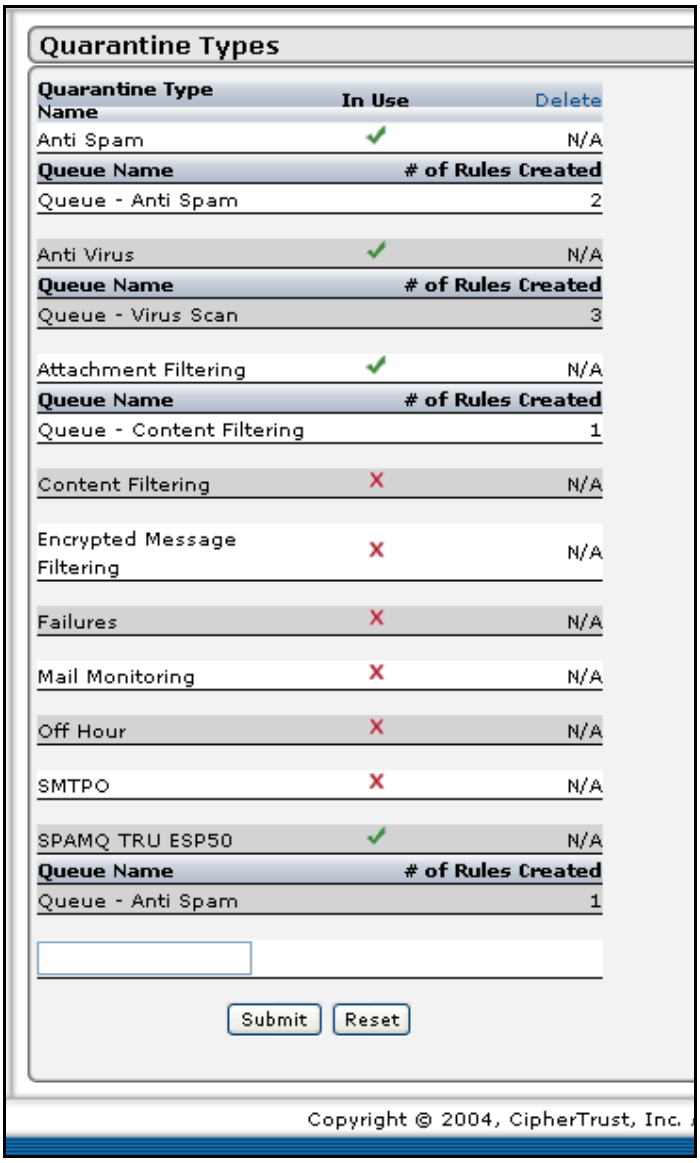


Quarantine Types

By default, IronMail provides the following quarantine queues:

- Content Filtering
- Attachment Filtering
- Mail Monitoring
- Anti Virus
- Encrypted Message Filtering
- Outbound (SMTPO Service)
- Anti-Spam
- Off Hour

Whenever an email *policy* configured with a "quarantine" action is created, administrators may specify to which quarantine queue the policy sends the message. This greatly eases the management of IronMail's policies—administrators can look in one place to see the results of that policy, without the interference of other messages that may also be quarantined. In addition to using the default quarantine queues, administrators are encouraged to create their own, even more "granular," quarantine queues. For example, when testing a new policy, the administrator might set the quarantine action to "send to the 'test' quarantine queue." As messages accumulate in that queue, the administrator can see exactly how effective the policy is—or is not.



The Quarantine Type page provides two types of user input:

Quarantine Type Name	This column lists the quarantine types by name. The default quarantine names are shown above.
In Use	Place a checkmark in the check box beside each type to be used by IronMail.
Delete	Select a manually-created quarantine queue's **Delete** check box to delete it from this table and from IronMail's queue architecture. (IronMail's default quarantine queues cannot be deleted.) The user is not allowed to delete a user-defined quarantine type so long as there are messages in the *associated queue*, or even when there are no messages but the quarantine type is used for a *rule*. You must first disable or delete the rule and/or release all messages, then delete the quarantine type.
New Type	If you want to add a new quarantine type, enter a name for that type in the data field at the bottom of the screen. Click **Submit**.

Note that if a manually-created quarantine queue is currently used by an IronMail policy, and the queue is deleted here, the policy is automatically modified to quarantine affected messages to the default queue in which the policy was created. For example, if a Mail Monitoring policy affects a message, but the manually-generated quarantine queue it was supposed to go to is deleted, IronMail will send those messages to the system-default Mail Monitoring Quarantine Queue. And if an Attachment Filtering policy was designed to send a message to a user-defined quarantine queue, and the queue is deleted, IronMail will automatically modify the policy so affected messages are delivered to the Content Filtering Quarantine Queue.

It is still possible to search quarantined messages or to release quarantined messages after the original queues have been deleted.

Refreshing the Queue Information Data

IronMail refreshes the Queue Information page automatically every *nnn* minutes—where *nnn* is the number of minutes entered in *System > Web Admin > Configure > "Auto Refresh."* To refresh the page manually, click the **Queue Information** hyperlink in the left navigation frame of the Web Administration interface.

Using the Quarantine Queue

The Quarantine Queue (and its subordinate user-defined quarantine queues) is one of the most functional parts of IronMail's "queue architecture." Its purpose is to allow the testing of email policies, visual verification that a message is spam, and a way to temporarily hold messages on disk without deleting them.

Use a quarantine queue to test an IronMail *policy* by configuring the policy's action to "quarantine" messages to a "testpolicy" quarantine queue. Allow IronMail to enforce that policy for one to two hours or days. When messages begin appearing in the "testpolicy" quarantine queue, verify that the intended messages are being detected.

One of the most critical elements of an anti-spam strategy is creating a whitelist of legitimate email addresses and domains that IronMail's spam-blocking tools "think" are generating spam. Configure the spam-blocking tools to quarantine suspected spam messages to a "spam" quarantine queue for several days. Administrators may visually inspect the contents of that quarantine queue for the presence of "false positives," and thus begin developing a whitelist. For even finer granularity, consider creating separate quarantine queues for User Defined Header Analysis, System Defined Header Analysis, and any other spam tools being tested. Configure their actions to quarantine suspected spam to their respective quarantine queues. In this way, it is easy to know exactly which messages (and/or false positives) each tool is detecting.

And finally, many administrators in high-volume email environments (50,000+ messages per day) will configure anti-spam or content filtering policies to quarantine messages for three to five days, and be deleted automatically afterward. When daily mail volumes make the visual inspection of the quarantine queue impractical, this approach allows administrators to search for messages if end users ask about them, and "push" out of the quarantine queue those messages that were inadvertently stopped. (Those domains or addresses may then be whitelisted, if appropriate.)

Consolidated Quarantine Server

Rather than storing quarantined messages in their various queues on the individual IronMail appliances, enterprises with multiple IronMails may opt to set up a Consolidated Quarantine Server (CQS) in the SuperQueue Service Properties screen by enabling its use and providing its IP address. This is a separate IronMail appliance uniquely equipped and configured for the sole purpose of storing quarantined messages. The CQS requires abundant memory in order to maintain messages coming from the other appliances for an acceptable amount of time.

To use the CQS, the other IronMails should be configured with a Forward Message action to send "quarantinable" messages to the CQS. The CQS will sort the messages and store them just as they would have been stored on the individual appliances.

Note: In order to work properly, the CQS must have all the IronMails that feed messages to it listed on its Allow Relay List. Furthermore, in order to process the forwarded messages as they would have been quarantined by the original IronMails, the CQS must have the same manually-created Quarantine Queues as the feeding IronMails, and the same processing order (queue order) and policy configuration as the individual appliances. They must all be configured to process messages using the same rules and policies.

SECURE COMMUNICATION

Overview

Current protocols governing email dictate that all messages transmitted over the internet be sent in plain ASCII text characters. The problem caused by this requirement is that anyone with the right tools can read a message sent by anyone else. The tools, such as TCP or *packet* sniffers, may be feely downloaded from the internet. The tools not only allow hackers to read anyone's email, but also allow them to intercept and alter the messages before they are delivered to the recipient. The easiest and most popular way for enterprises to secure their email is by using Digital Certificates.

These certificates allow two essential strategies for message encryption: "client to client" and "server to server" encryption. In client-to-client encryption, Security Certificates are installed on individual workstations. The dominant benefit of this method is that the message is encrypted before it leaves the originator's computer and remains encrypted until it is received (protection from end to end). Server-to-server encryption, on the other hand, requires Security Certificates be installed on the mail servers. Messages are protected only from server to server, not from the client to the server. The following comparison illustrates the differences.

Problem Area	Client-to-Client	Server-to-Server
Expense	Certificates must be purchased for and installed on every individual computer that will send and receive encrypted mail.	Only one certificate must be installed on the server; one server can encrypt and protect all email for client PCs in the domain.
Administrative Workload	All certificates must be updated regularly, and may need to be uninstalled or transferred from one computer to another.	Administrators must manage only one certificate per gateway.
User Workload	Each user must tell all mail clients to user the certificates.	Encryption is transparent to the end user, and users cannot disable the encryption.
Scanability	Messages are encrypted before they reach the gateway. Therefore, they cannot be scanned for viruses, malicious content or confidential information, nor can the be scanned at the receiving gateway.	Messages may be scanned for viruses, spam, and email policy enforcement.
Encryption Security	Message body is encrypted, but header and routing information is not. Hackers have the opportunity to gain helpful information, and may be attracted by the encryption of the message body.	Establishes a secure tunnel between the sending and receiving email servers. Routing and encryption information is hidden.

IronMail's strategy provides the benefits of server-to-server encryption without permitting its drawbacks.

IronMail Security Strategy

IronMail provides an interface for requesting and installing a Security Certificate from a Certificate Authority. When a certificate is installed on the IronMail appliance, it is not necessary to install addtional certificates on internal servers, unless the Administrator wants to protect the connection

between IronMail and the internal servers and provide security for internal users sending or retrieving messages directly to or from the server. IronMail requires the installation of a Security Certificate so that administrative sessions with it via the Web Administration browser interface can be conducted securely.

For server to server encryption, IronMail includes a single option in the Mail-VPN configuration that tells it to always try to send messages securely over Port 25 (SMTPS). You can also instruct IronMail what to do if the receiving server doesn't accommodate a secure session. IronMail can fall back to non-secure delivery or it can be configured not to send the message at all.

IronMail is capable of creating the secure tunnel for messages, and also allows creation of policies for with whom you may or may not establish the secure tunnel. IronMail's Policy Manager allows you to create lists of domains to which you always send encrypted messages and those to which you never send them. In addition, the Administrator can create Mail Virtual Private Networks between domains.

For client to server encryption, IronMail allows users to configure their email applications to send and retrieve mail securely over port 465 (for SMTPS), port 993 (for IMAP4S) or port 995 (for POP3S). The email applications then use IronMail's Security Certificate to encrypt messages. IronMail can also send messages securely over the standard port 25.

If you want to secure messages between the internal mail server and the IronMail appliance, an option in IronMail's POP3S and IMAP4S configuration tells IronMail to request a secure connection.

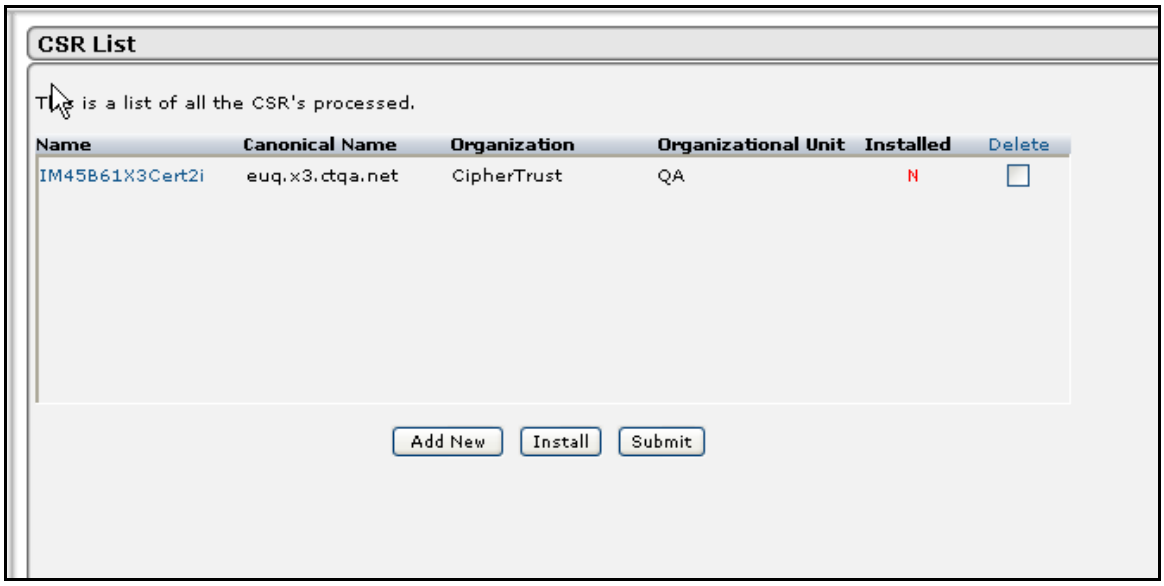
Managing Certificates

Certificate Manager

IronMail protects messages in transit through the use of various methods to either create encrypted channels of communication (*SSL*) or encrypted message data (S/*MIME* or PGP). When IronMail is first installed, it is delivered with a "self-signed" Security Certificate which is adequate for encrypting the Web Administration sessions for administrators managing their IronMails. This self-signed certificate can also encrypt SMTP messaging, though sending servers may refuse to deliver their email to a server whose certificate cannot be authenticated. Therefore, administrators are enabled by IronMail to create and install certificates signed by a certificate authority. This Certificate Manager program area provides the ability to create a "Certificate Signing Request," as well as to install, backup and restore one or more Security Certificates.

Generate CSR

IronMail requires the use of Security Certificates to provide secure services, much like banks or e-commerce web sites use them to provide secure connections for their web customers. The Certificate Signing Request (CSR) is actually the request made by an Administrator for a new certificate. Open the CSR List to see existing CSRs and to request new ones (Secure Delivery > Certificate Management > X509 Certificates > CSR List).



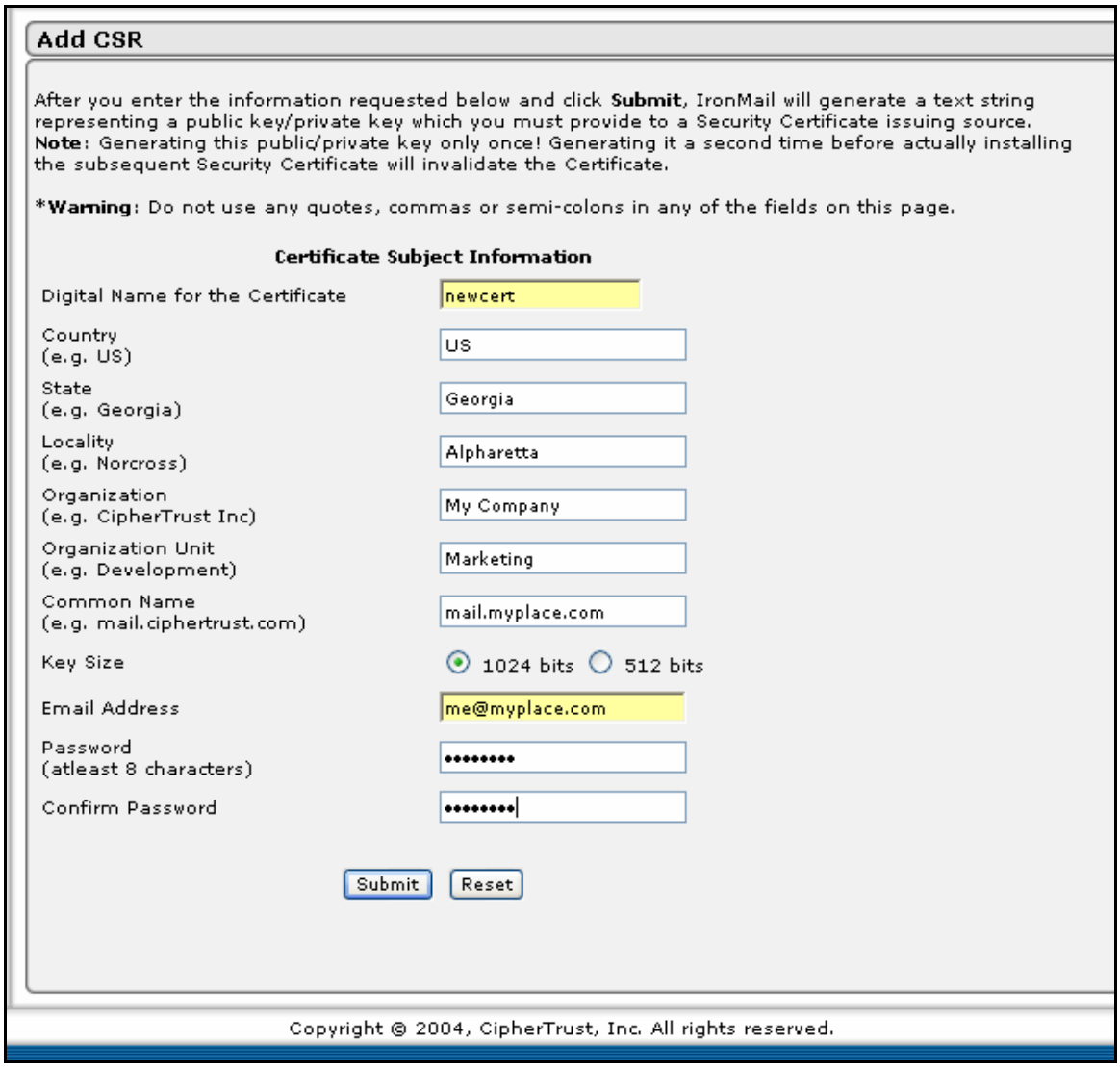
The CSR List screen displays the following information:

Field	Description
Name	This column shows the digital name for each CSR that has been processed and is awaiting installation.
Canonical Name	This column displays the canonical name for the server where the certificate will be installed. Example: mail.marketing.myplace.com
Organization	The name of the organization (e.g., CipherTrust, Inc.) that requested the CSR shows in this column.
Organizational Unit	This column lists the department or unit within the organization to which the certificate will be assigned (e.g., Development).
Installed	This column contains an N (for "not installed") until the certificate is installed.
Delete	Clicking the delete checkbox associated with any CSR and clicking **Submit** will delete that CSR. Clicking the Delete hyperlink will delete all CSRs.

Click **Submit** to record any action.

Adding a CSR

Clicking the Add New button at the bottom of the CSR List screen opens the following window. If administrators do not already possess a valid Security Certificate for the IronMail, the first step is to first generate a Certificate Signing Request by filling in the input fields in this window


Add CSR
After you enter the information requested below and click Submit, IronMail will generate a text string representing a public key/private key which you must provide to a Security Certificate issuing source.
Note: Generating this public/private key only once! Generating it a second time before actually installing the subsequent Security Certificate will invalidate the Certificate.
*Warning: Do not use any quotes, commas or semi-colons in any of the fields on this page.
Certificate Subject Information
Digital Name for the Certificate
newcert
Country (e.g. US)
US
State (e.g. Georgia)
Georgia
Locality (e.g. Norcross)
Alpharetta
Organization (e.g. CipherTrust Inc)
My Company
Organization Unit (e.g. Development)
Marketing
Common Name (e.g. mail.ciphertrust.com)
mail.myplace.com
Key Size
1024 bits
512 bits
Email Address
me@myplace.com
Password (atleast 8 characters)
Confirm Password
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

Field	Description
Digital Name for the Certificate	Enter the digital (displayed) name for the new certificate being requested.
Country	Enter the name or abbreviation for the country where the certificate is to apply.
State	Enter the state name.
Locality	Enter the name of the locality.
Organization	Enter the name of the organization requesting the certificate.
Organization Unit	If applicable, enter the name of the unit within the organization to which the certificate will be assigned.

Common Name	Enter the server name where the certificate will be installed.
Key Size	Select the appropriate key size, in bits, for the public key to be installed. Options are: • 1024 bits • 512 bits The larger key is more secure, but is slower to process.
Email Address	Enter the email address for the Administrator for the certificate.
Password	Enter the password to be used by the Administrator to maintain the certificate.
Confirm Password	Confirm the password by entering it again.

Click **Submit** to create the request. The CSR will be added to the CSR List.

IronMail will generate a private key/public key pair, and display in a text string the public key to be submitted to a "trusted root" source (such as VeriSign) for Security Certificates. Open a second browser window to navigate to a Security Certificate-issuing source.

Copy and paste the IronMail-generated text string into the appropriate input field of the Certificate Authority's web page when applying for a Certificate. When copying and pasting the key information, include the

"- - - - -BEGIN CERTIFICATE REQUEST- - - - -" AND "- - - - -END CERTIFICATE REQUEST- - - - -"

at the beginning and end of the IronMail-generated text string.

When you go to the Verisign web page to get your certificates, you will be asked what platform you plan to use. Select **Apache**. If you choose Windows or IIS, the certificates you download will not work with IronMail appliances.

When you click **Submit**, the CSR is submitted to the Certificate Authority (CA). IronMail creates and stores a private key/public key text string in its database. When this string is submitted to a CA after the administrator completes and submits the CSR a *second* time, the issuing authority generates a new public key string. The new certificate information appears in the CSR List.

The install procedure allows you to paste this string in the IronMail Certificate section of the Install Security Certificate window and complete the certificate generation.

Types of Certificates

IronMail supports two primary certificate types: X.509 certificates and PGP certificates. Each type provides encryption standards that IronMail will use to send and receive messages. X.509 certificates use both a public key - shared with others that will be allowed to send encrypted messages to IronMail or receive encrypted messages from IronMail - and a private key that is maintained in complete secrecy. The private key is used to encrypt outgoing messages and decrypt incoming messages. The certificates must be purchased from a Trusted Root Certificate Authority (CA).

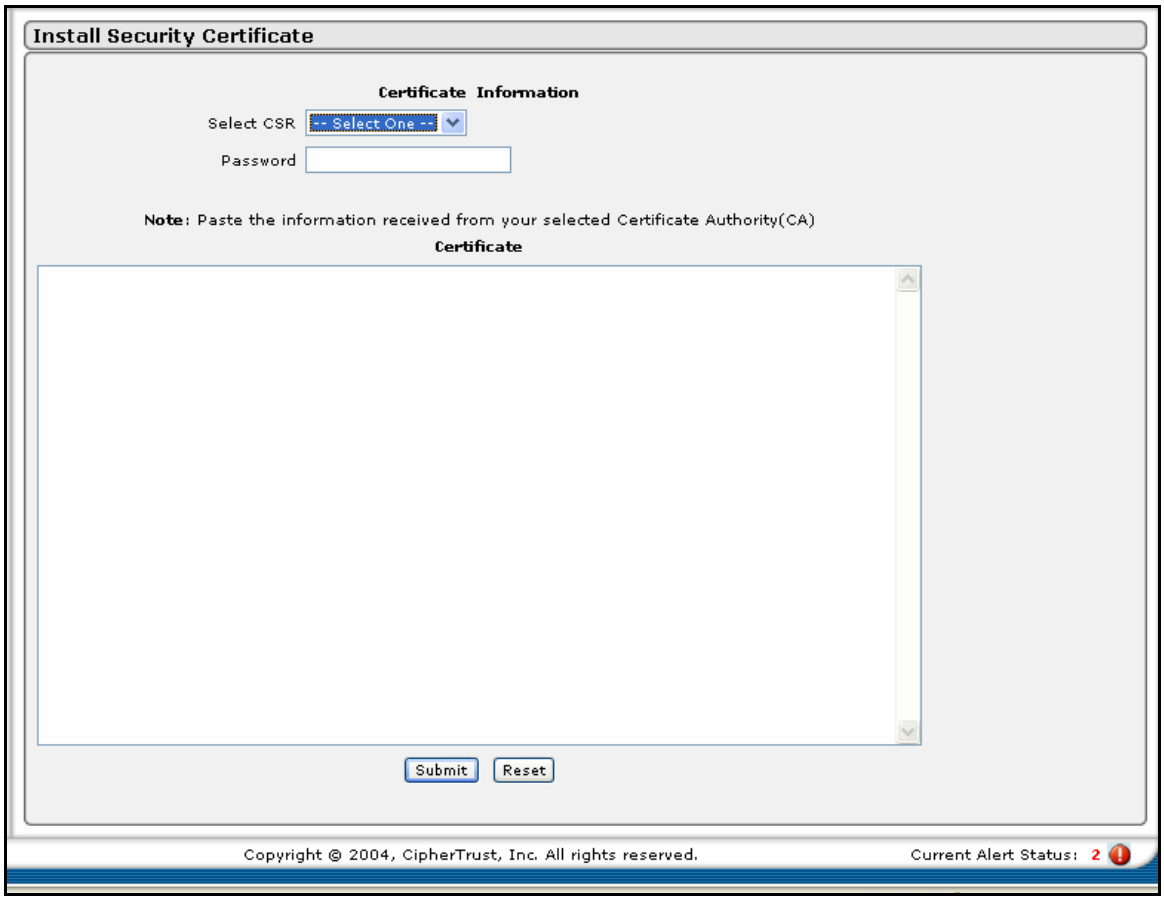
PGP certificates also uses the public and private keys, but rather than binding the certificate to the user (or server), PGP uses a Web of Trust concept, a multiple path of certification that allows some tolerance. The PGP certificates are generated by a PGP encryption package, available free from several sources. The official repository is at the Massachusetts Institute of Technology.

X.509 certificates are used for IronMail's S/MIME functionality.

Installing X.509 Certificates

IronMail is pre-configured with an unsigned certificate in order to immediately provide secure *SSL* connections required for administrative sessions with the Web Administration interface. While the invalid certificate does allow encryption of email messages, that security is minimal because IronMail will not be able to authenticate itself to other servers, which may refuse to send messages to it. Therefore, in order to provide genuine security, a valid Security Certificate must be installed.

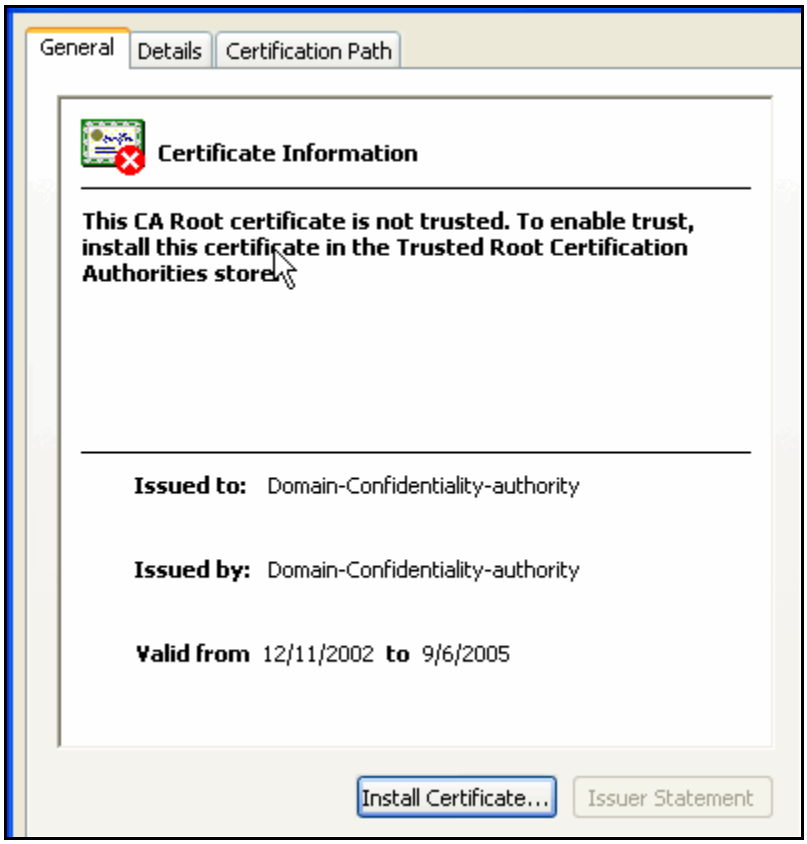
When the Certificate Authority returns the necessary certificate information, click Install on the CSR List screen. The Install Security Certificate window opens.



From the picklist, populated from the CSR List, select the certificate that is to be installed. Enter the password that was used to request the CSR from the Certificate Authority (CA). Then copy and paste into the Certificate input field the Security Certificate text string provided by the CA. Click **Submit**. The certificate will be installed, and the CSR will disappear from the CSR List.

To verify that the Security Certificate is installed correctly, double-click the “lock symbol” in the Status Bar of the Web Administration browser window.

A Certificate Properties window is displayed, providing information about the Certificate. If the Certificate is invalid, this Properties window may display the following:


General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Domain-Confidentiality-authority
Issued by: Domain-Confidentiality-authority
Valid from 12/11/2002 to 9/6/2005
Install Certificate...
Issuer Statement

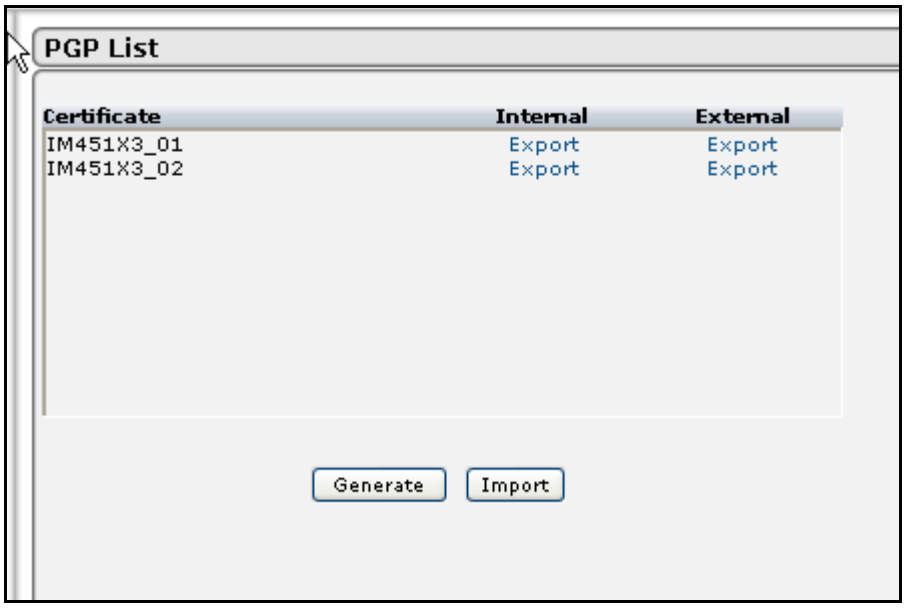
(There will never be an instance in which there is no lock icon in the Status Bar. Without IronMail's default invalid Security Certificate at the very least, IronMail won't launch.)

Note: Installed Security Certificates cannot be uninstalled.

Storing Certificates

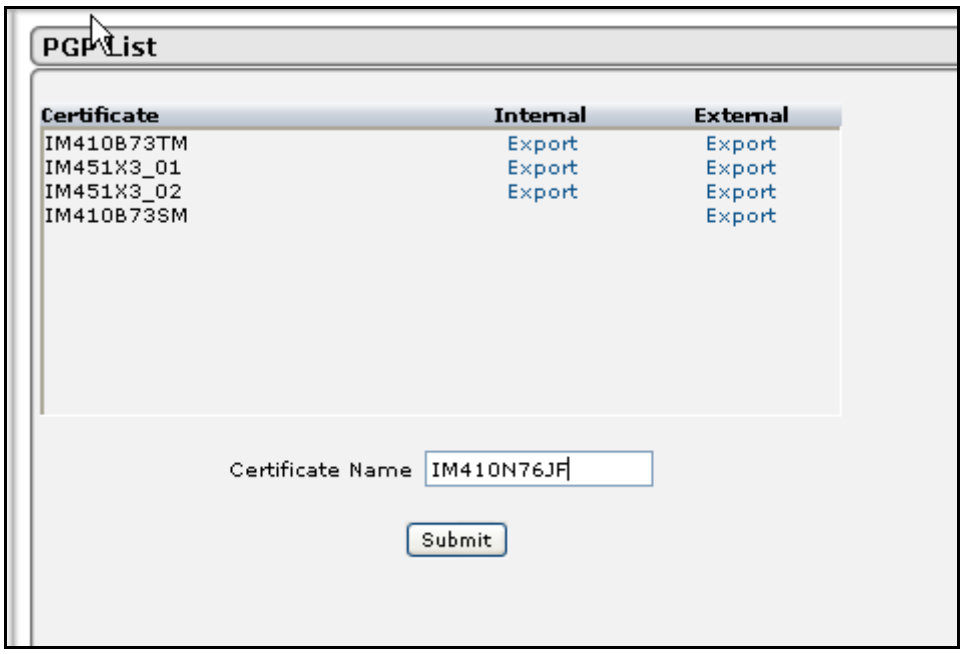
When a certificate is installed, it is added to the storage lists (X509 List or PGP List) Storing the available certificates (either X.509 or PGP) allows them to be archived for backup purposes. X.509 Certificates are added from the CSR list when they are installed.

Similarly, all PGP Certificates appear in the PGP List. This screen is also used for generating PGP certificates.

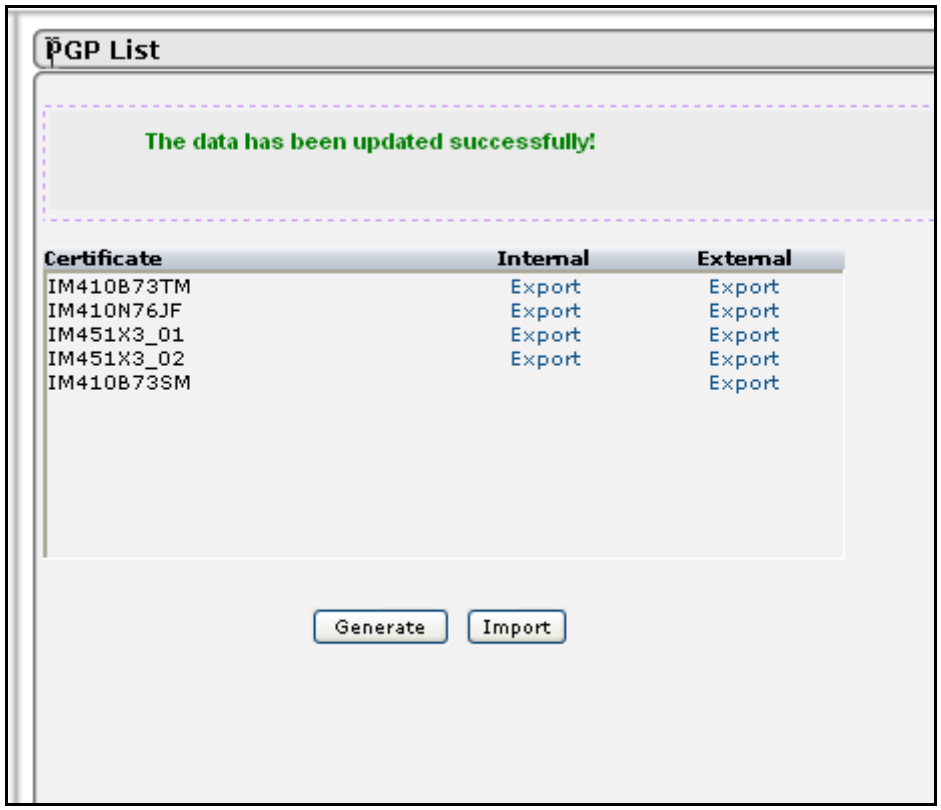


Generating PGP Certificates

To generate and install a new PGP certificate, click the **Generate** button. The screen changes to allow entry of a new certificate name. The PGP key is associated with a specific domain hosted by IronMail, and which requires PGP encryption.



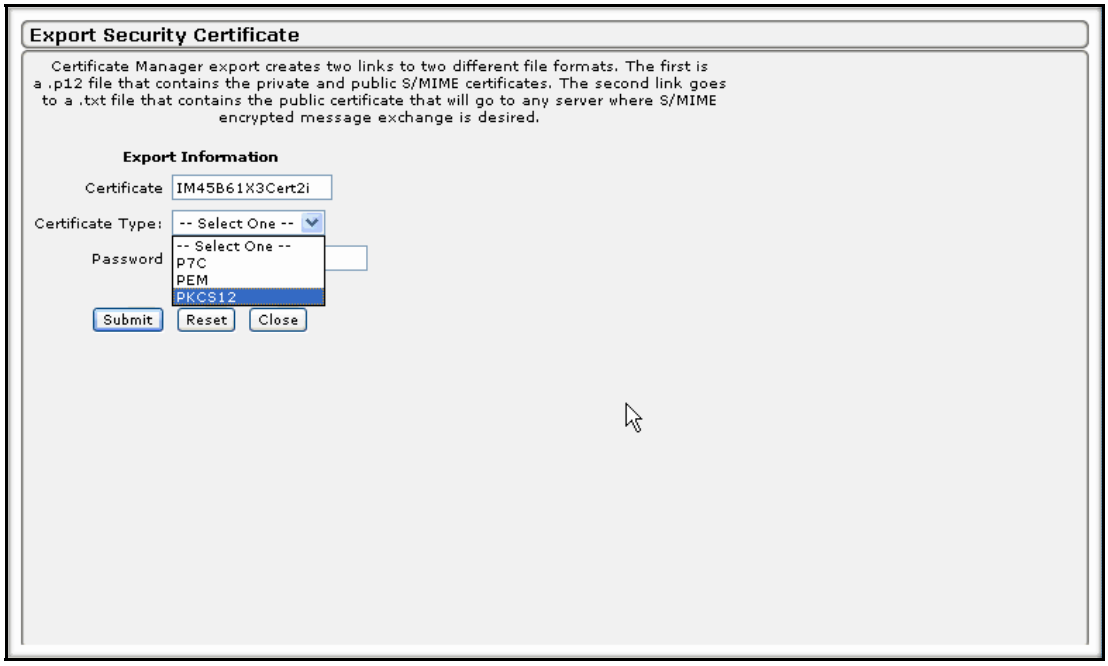
Enter the certificate name and click **Submit**. The new certificate is added to the list and installed on the IronMail appliance.



Exporting Certificates

Because the Security Certificate may cost a considerable sum of money, IronMail provides a mechanism allowing administrators to "archive" a copy of it for safekeeping. Additionally, the public key of installed *SSL* and S/*MIME* Security Certificates may be exported to disk so they may be shared with trusted domains.

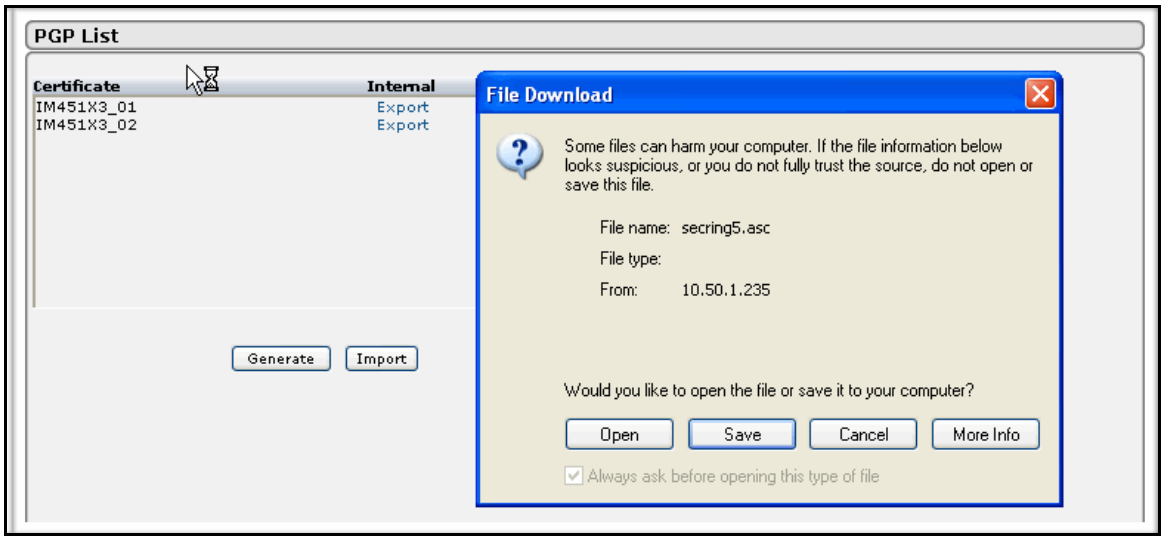
Exporting from certificate storage in the X509 List:


Export Security Certificate
Certificate Manager export creates two links to two different file formats. The first is a .p12 file that contains the private and public S/MIME certificates. The second link goes to a .txt file that contains the public certificate that will go to any server where S/MIME encrypted message exchange is desired.
Export Information
Certificate
IM45B61X3Cert2i
Certificate Type:
-- Select One --
-- Select One --
P7C
PEM
PKCS12
Password
Submit
Reset
Close

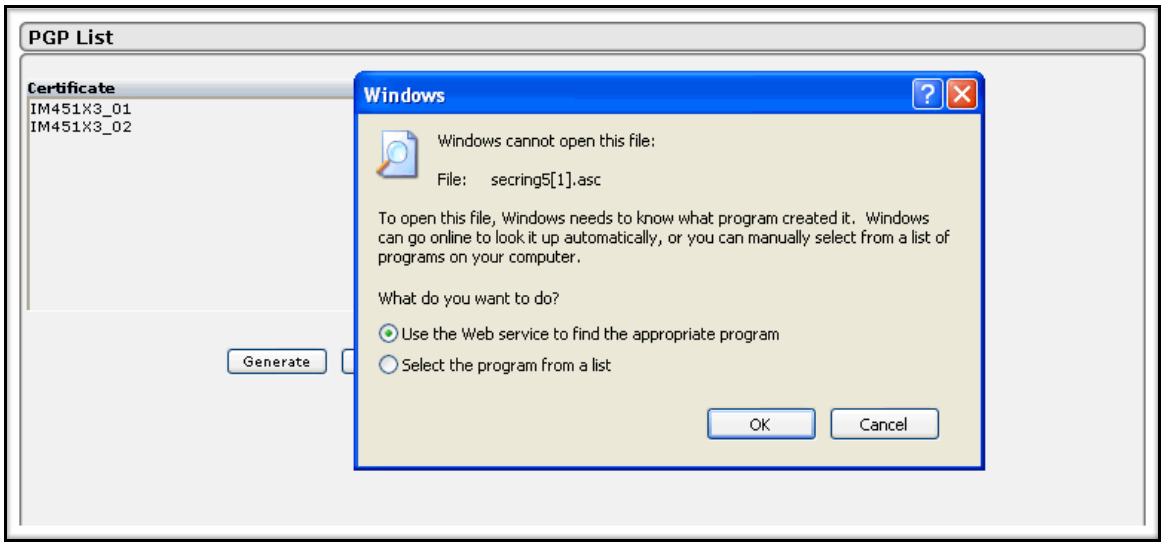
Field	Desription
Certificate	Enter the name of the certificate to be exported.
Certificate Type	From the pick list, select the certificate type. Options are: • P7 - This contains the *public key* of a selected X509 Security Certificate in "P7C" format. This file may be shared with other domains to provide for message encryption. The domain's server will specify which format is required. • PEM - This contains the *public key* of a selected SSL or S/MIME Security Certificate in "CER" format. This file may be shared with other domains to provide for message encryption. • P12 - This file contains both the private key and public key of the Certificate in a format required for installing on another IronMail appliance. *Never distribute this file to another domain!*
Password	Enter the password used to request the certificate. This password will also be used to import the certificate if that becomes necessary.

Click **Submit** to export the certificate.

To export from the PGP List, simply click the Export hyperlink under either Internal or External headings. The resultant screen appears as below.



You may save the file to your computer or open it. Clicking Open results in the following screen.


PGP List
Certificate
IM451X3_01
IM451X3_02
Generate
Windows
Windows cannot open this file:
File: secring5[1].asc
To open this file, Windows needs to know what program created it. Windows can go online to look it up automatically, or you can manually select from a list of programs on your computer.
What do you want to do?
Use the Web service to find the appropriate program
Select the program from a list
OK
Cancel

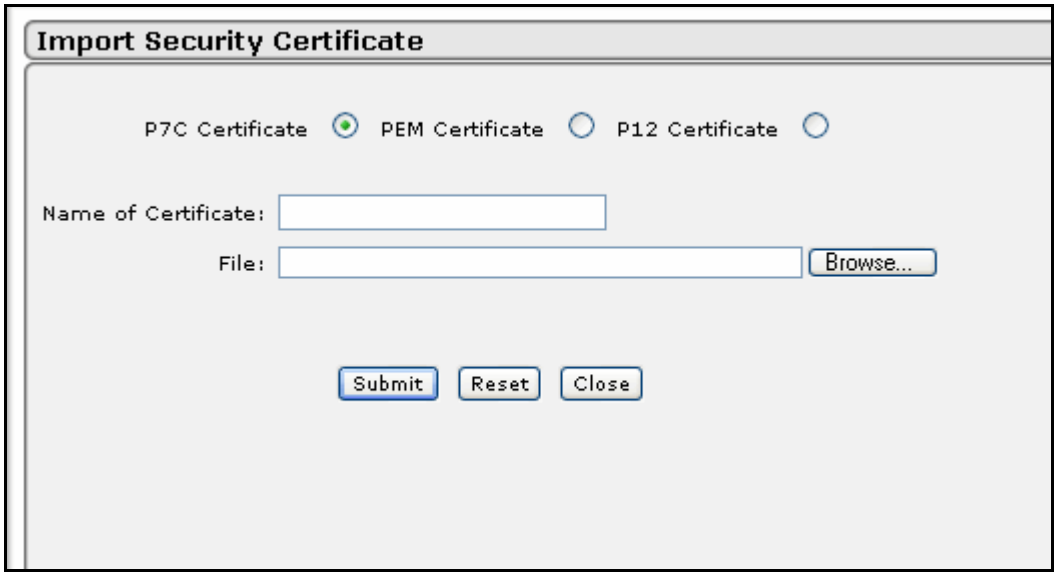
- **PKCS 12 Format File:** Clicking this hyperlink opens a Save As dialog where the file may be saved to disk.
- **Certificate File (first):** The domain's server will specify which format is required. Clicking this hyperlink opens a Save As dialog where the file may be saved to disk.
- **Certificate File (second):** Clicking this hyperlink opens a Save As dialog where the file may be saved to disk.

Importing Certificates

Administrators may import a previously exported IronMail Security Certificate for installation on a new machine or for restoration purposes.

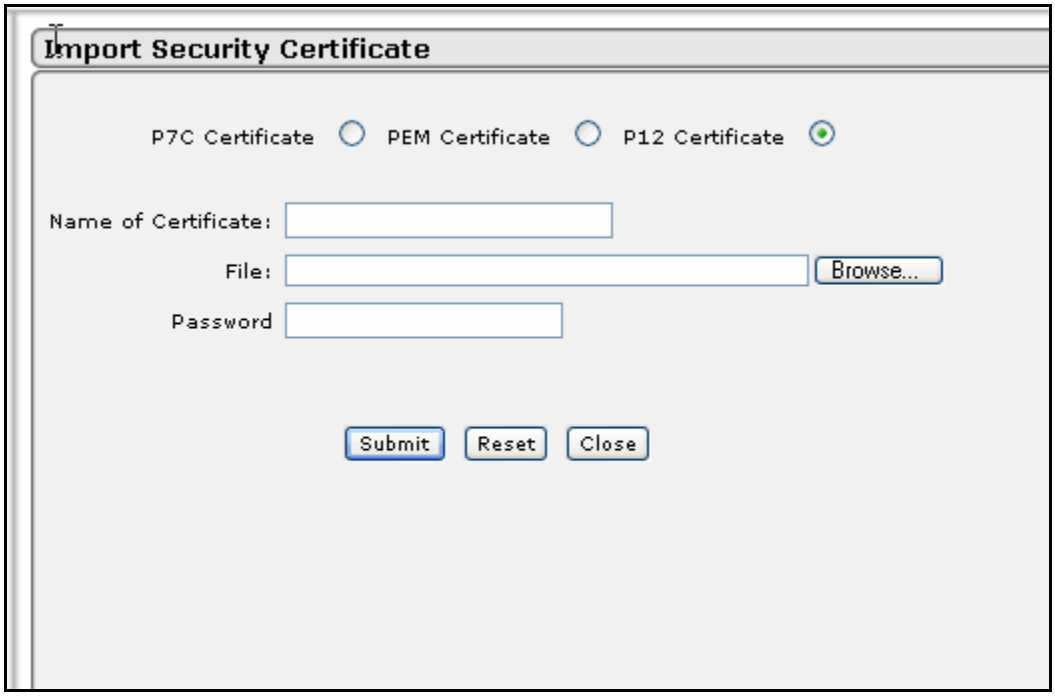
Importing X.509 Certificates

To import an X.509 certificate, click the Import button at the bottom of the X509 List screen. The Import Security Certificate screen displays.



The specific screen to use will depend upon what type of X509 certificate you want to import. The screen for the P7 Certificate is shown above. The PEM and P12 screens appear below. Note: P7C

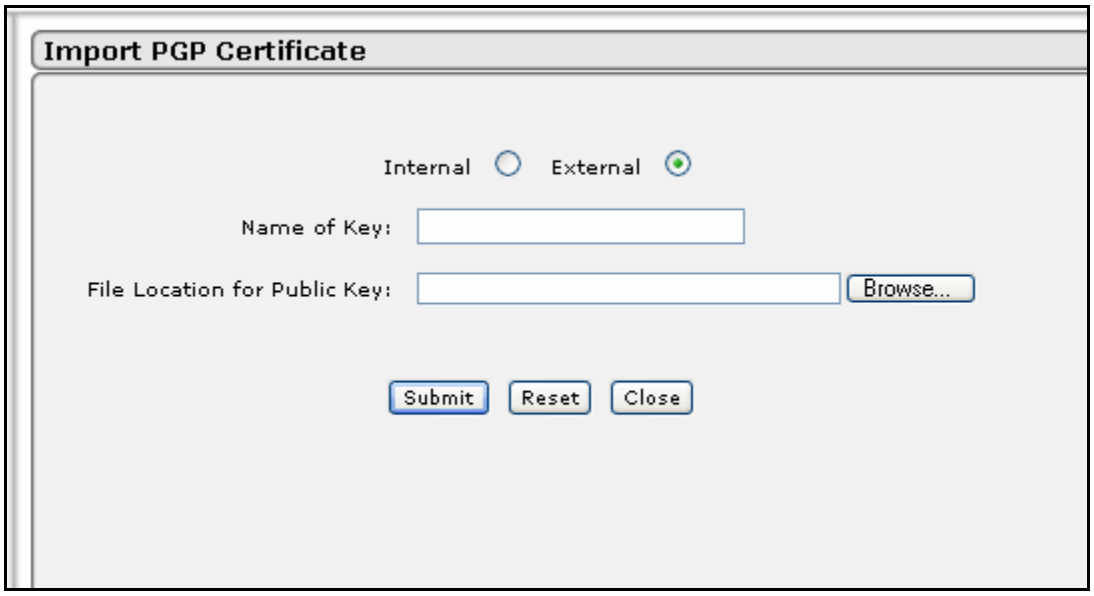
and PEM Certificates involve public keys only. No password is required. Simply enter the information required, browse to the file location where the certificate is stored (for P7C) and click **Submit**.



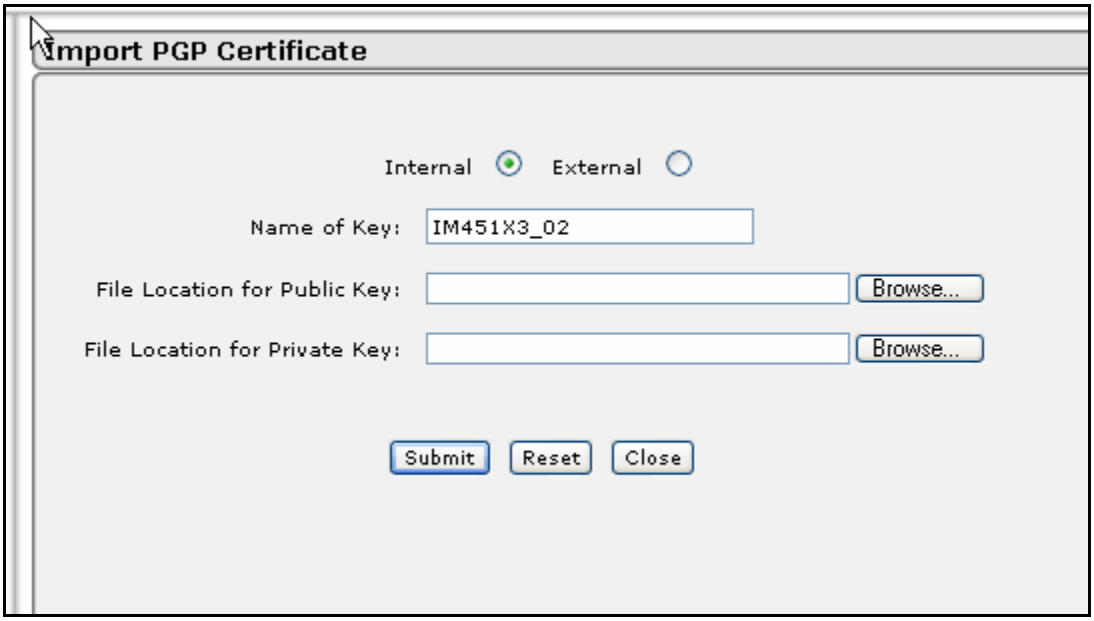
For the P12 Certificates, a password is required, since the certificate contains both public and private keys. Enter the certificate name, browse to the file storage location, and enter the password that was associated with the certificate at the time it was exported. Click **Submit**. The imported certificate will appear on the X.509 List.

Importing PGP Certificates

To import a PGP certificate, click the Import button at the bottom of the PGP List screen. The Import PGP Certificate screen opens.



Just as with X.509 certificates, the actual screen to be used for importing the certificate will depend upon whether you want to import the internal or external version. The screen for the External (public) key is shown above. To import, enter the name of the key, browse to the storage location and click **Submit**.



To import the Internal certificate, the additional step of browsing to the private key location is shown. Click **Submit** to import the certificate. The certificate will appear on the PGP List.

Configuring Mail Certificates

This screen is used to select the X.509 Certificate IronMail will use for SSL encryption. All installed X.509 certificates will show on the pick list. The Administrator selects one from the pick list and clicks **Submit**.

onfigure Certificate
All X.509 Security Certificates that have been installed on IronMail appear in the pick list. Select the one IronMail should use for SSL encryption of SMTP, POP3, and IMAP4 email. ("Default" in this list refers to the invalid certificate that is installed by default to allow for Web Administration.)
Select Certificate:
DEFAULT
Submit
Reset

Although this function may be logically seen as part of Certificate Management, the screen is actually located under Administration (Administration > Configure Mail Certificates).

Secure Delivery

Secure Delivery

IronMail Secure Delivery is a system of encryption tools, filters and email policies. It includes:

- Mail-VPN, using *SSL*/TLS to create a secure connection to the recipient server or client and to deliver the message securely. Mail-VPN requires support for SSL/TLS on the recipient server or client.
- Server-side S/MIME, one of two major secure key exchange standards. Server-side S/*MIME* is used primarily to support legacy encryption systems.
- Server-side PGP, the other major secure key exchange standard. Server-side PGP functionality is used mainly to support legacy encryption systems.
- Secure Web Delivery (SWD), used when a message must be delivered securely, but no secure connection can be established with the recipient server. This method emails the recipient that they have a message waiting in a secure, web-based mailbox. The notification provides a URL link to the secure web page where the message may be retrieved.

Additionally, when encryption is performed at the gateway, Secure Delivery allows the Administrator to use Content Filtering and Policy Manager to make decisions about encryption of messages, based on keywords or header information. Secure Delivery will attempt to deliver the message securely using any of the available methods as configured by the Administrator, with Secure Web Delivery as the final method. IronMail can be configured to "fall back" to SWD.

IronMail's Encrypted Message Filtering allows client-based encryption and digital signatures. These features can guarantee that email really came from the stated sender and that no one has altered the message. The drawback is that, just as this encryption protects the messages, it also protects viruses, malicious code and confidential information sent by unscrupulous employees.

The Boundary to Boundary screens for this Secure Delivery program area allow administrators to specify the domains for which IronMail shall require or deny the use of encryption, to manage the Security Certificates required by the encryption protocols.

Boundary to Boundary

The Boundary-to Boundary pages are used to configure the use of S/MIME, PGP, and SSL for specific domains, both for inbound mail *from* them and outgoing mail *to* them. The Boundary to Boundary hyperlink in the left navigation frame expands to offer External and Internal sub-menus. "External" denotes the external domains to which IronMail will be delivering email. "Internal" denotes that IronMail will be the recipient of messages arriving from external domains.

When internal users send outbound messages to the domains specified in these pages, IronMail will require or deny the use of encryption. The **External** hyperlink expands to offer S/MIME and PGP, sub-menus.

When internal users receive messages originating from domains specified in these pages, IronMail will require or deny the use of encryption. The **Internal** hyperlink expands to offer S/MIME and PGP sub-menus.

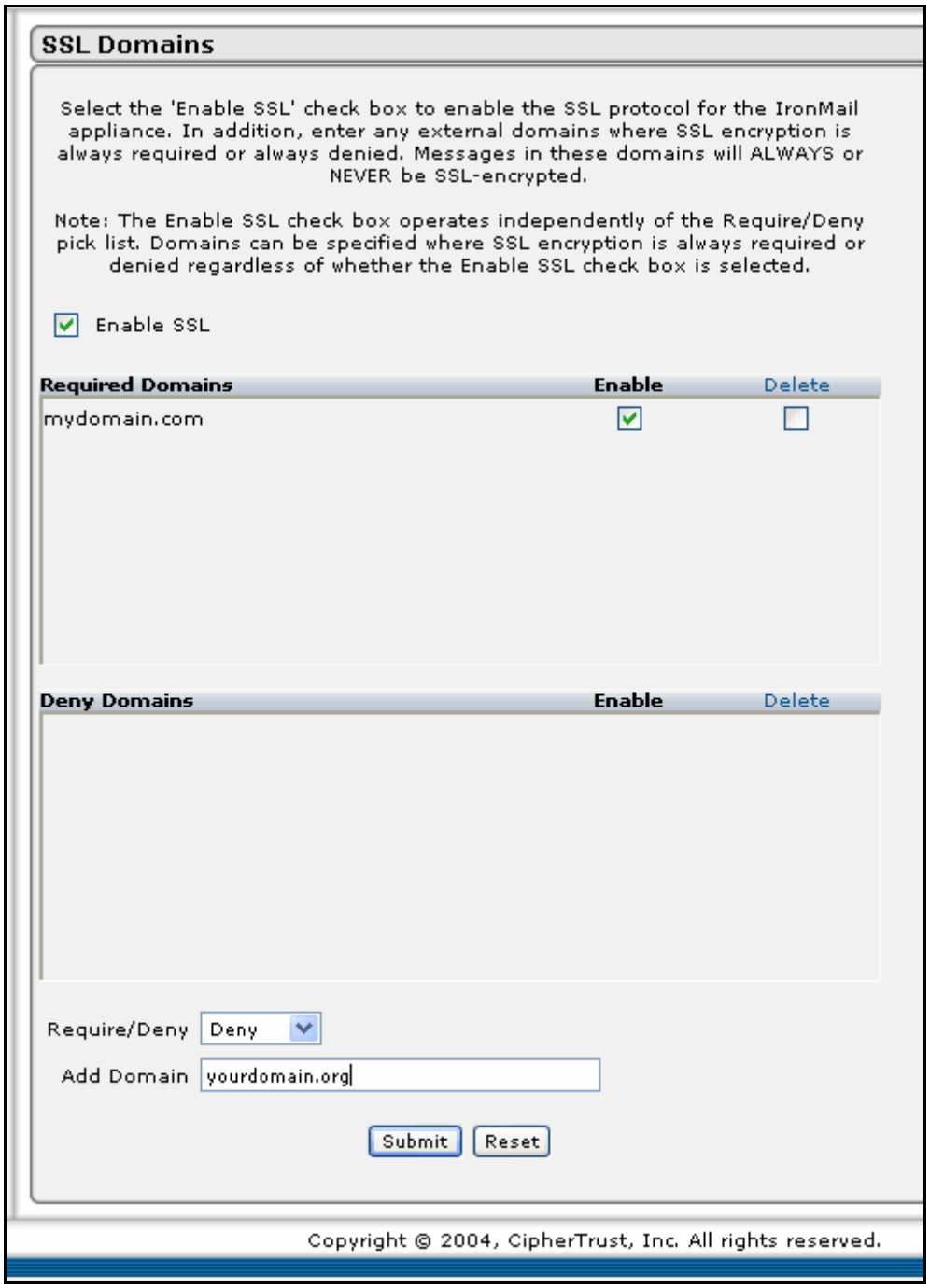
Configuring S/MIME- or PGP-encrypted email originating from these domains overrides the SSL setting that may be configured in the SMTPI Properties.

For IronMail to receive incoming messages securely, S/*MIME* and/or PGP Security Certificates must be installed on it for the given domains.

Note that if an S/MIME Security Certificate (X.509) is issued by a Certificate Authority (CA) whose name is not installed in IronMail, *the message will not be delivered.*

SSL

Use this page to enable the *SSL protocol* for IronMail appliances. In addition, the screen provides a **Require/Deny** pick list to add Required Domains where IronMail will only send messages to users in the domain securely, or to add Deny Domains where IronMail will never send SSL-encrypted messages.


SSL Domains
Select the 'Enable SSL' check box to enable the SSL protocol for the IronMail appliance. In addition, enter any external domains where SSL encryption is always required or always denied. Messages in these domains will ALWAYS or NEVER be SSL-encrypted.
Note: The Enable SSL check box operates independently of the Require/Deny pick list. Domains can be specified where SSL encryption is always required or denied regardless of whether the Enable SSL check box is selected.
Enable SSL
Required Domains
Enable
Delete
mydomain.com
Deny Domains
Enable
Delete
Require/Deny
Deny
Add Domain
yourdomain.org
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

Two tables on this page, empty until domains have been added, will show the domains for which SSL is required or denied.

Select the **Enable SSL** check box to enable this service.

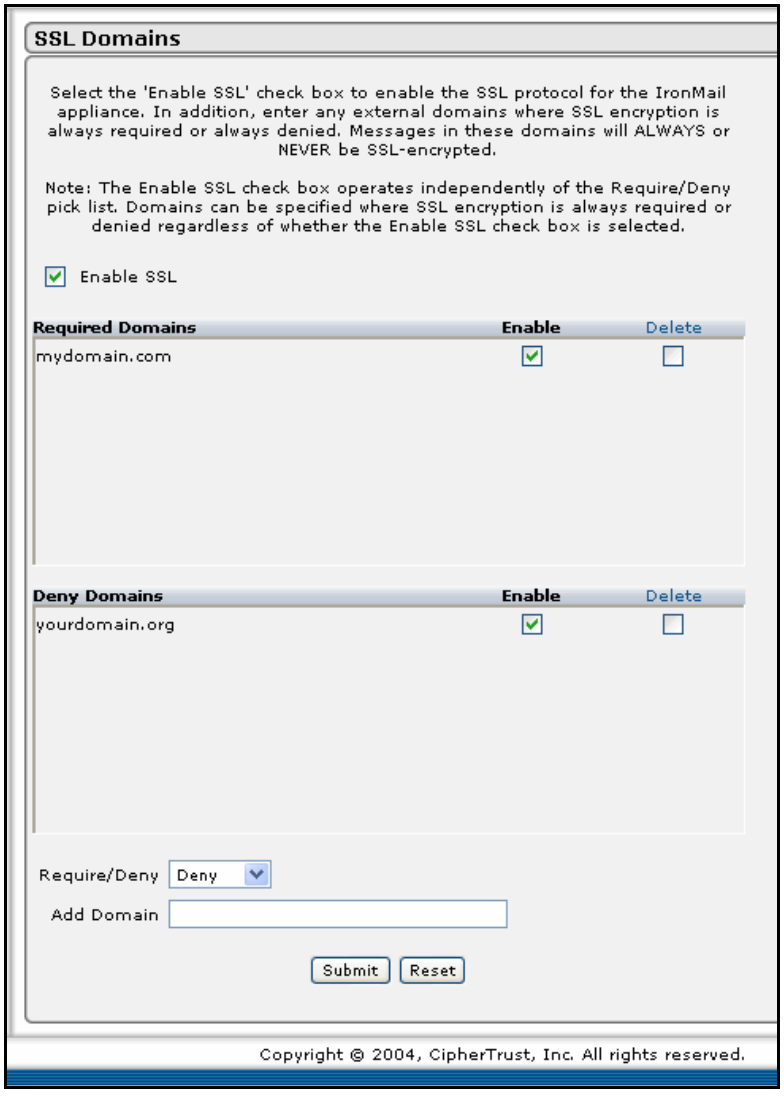
The two tables provide the following information:

Require/Deny Domains	This column will display the names of any domains for which SSL encryption is required or denied.
Enable	The **Enable** check box is selected by default when a domain is added to a table. To temporarily stop requiring or denying SSL encryption without deleting the domain from the table, de-select this check box.
Delete	Select a domain's **Delete** check box to remove a domain from the table, and stop enforcing the use of SSL.

Whenever internal users send messages to these domains, IronMail will attempt to establish a secure connection with the mail server in that domain. If the receiving server cannot support an SSL session for whatever reason, IronMail will drop the message or fall ack to Secure Web Delivery if it is configured to do so.

Adding or Editing Domains

Add a domain by entering the *domain name* in the data field and selecting "Require" or "Deny" from the pick list. Click Submit, and the window refreshes with the new domain in place.


SSL Domains
Select the 'Enable SSL' check box to enable the SSL protocol for the IronMail appliance. In addition, enter any external domains where SSL encryption is always required or always denied. Messages in these domains will ALWAYS or NEVER be SSL-encrypted.
Note: The Enable SSL check box operates independently of the Require/Deny pick list. Domains can be specified where SSL encryption is always required or denied regardless of whether the Enable SSL check box is selected.
Enable SSL
Required Domains
Enable
Delete
mydomain.com
Deny Domains
Enable
Delete
yourdomain.org
Require/Deny
Deny
Add Domain
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

The Administrator can enable, disable or delete a domain by clicking the appropriate check boxes and clicking **Submit**.

S/MIME

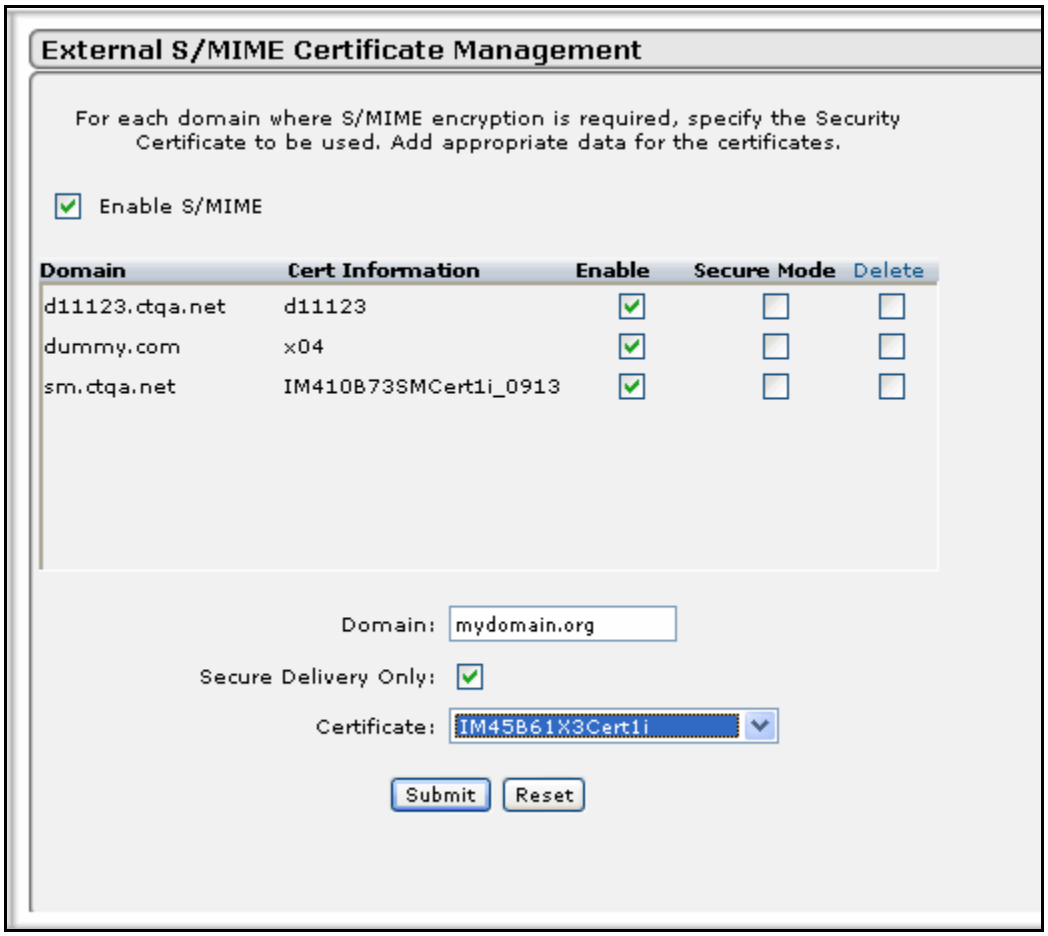
IronMail provides the ability to send and received server-based S/*MIME* messages using much the same functionality as Mail-VPN.

Every incoming message is checked to see if it is an S/MIME message. If so, IronMail checks to see if a key exists to decrypt the message. If a key exists, IronMail decrypts the message. If no key exists, the message is treated flows as normal, skipping specific queues, providing that *Policy* Manager has not been configured to block S/MIME messages to the specific user.

Outgoing messages are checked for a domain or user that exists in the S/MIME encryption list. Different keys are required for different domains.

External S/MIME

Use the S/*MIME* page to configure the domains that require S/MIME encryption. Note that the public key of the S/MIME Security Certificate of each external domain must be installed on the IronMail (See "Add New Certificate" below).

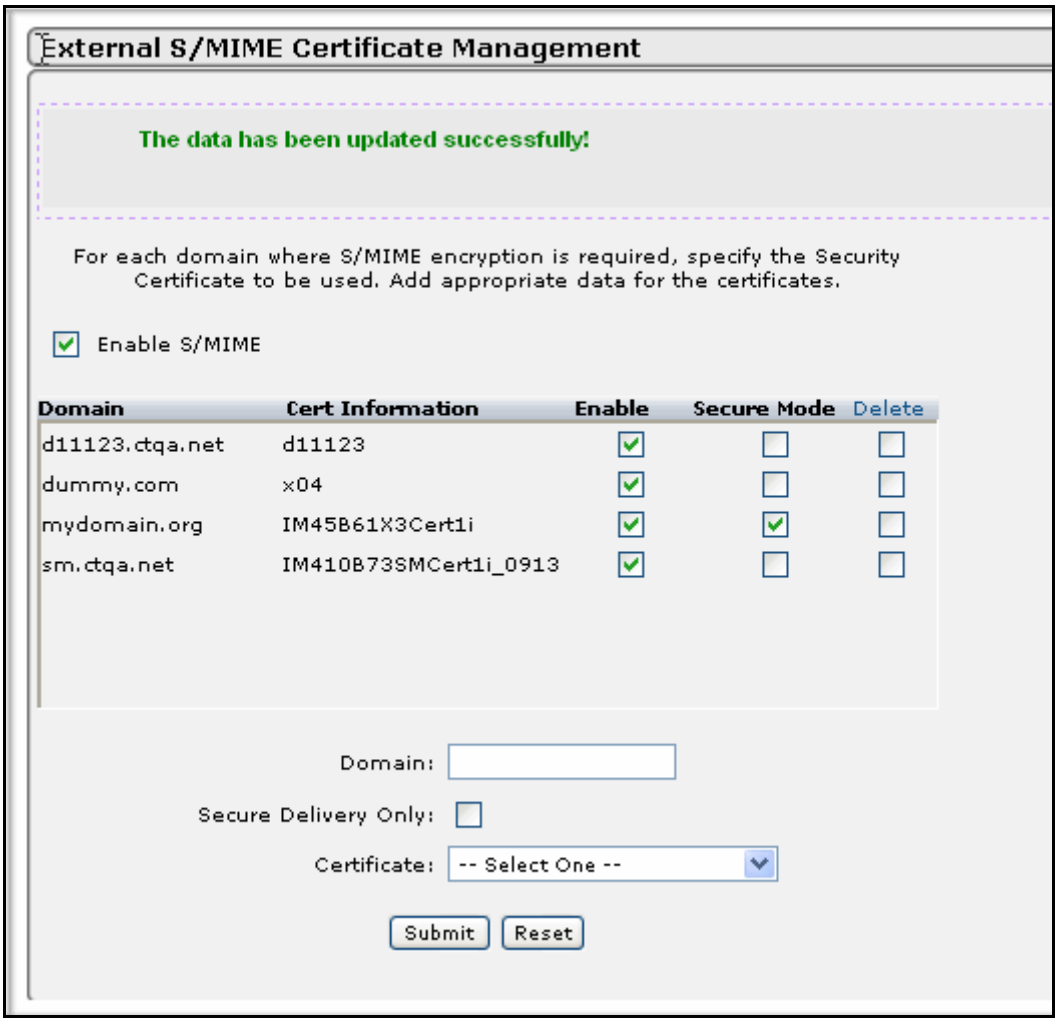


Select the **Enable S/MIME** check box to require IronMail to use S/MIME encryption when sending messages to the domains added to the table on this page.

The table of domains provides the following information:

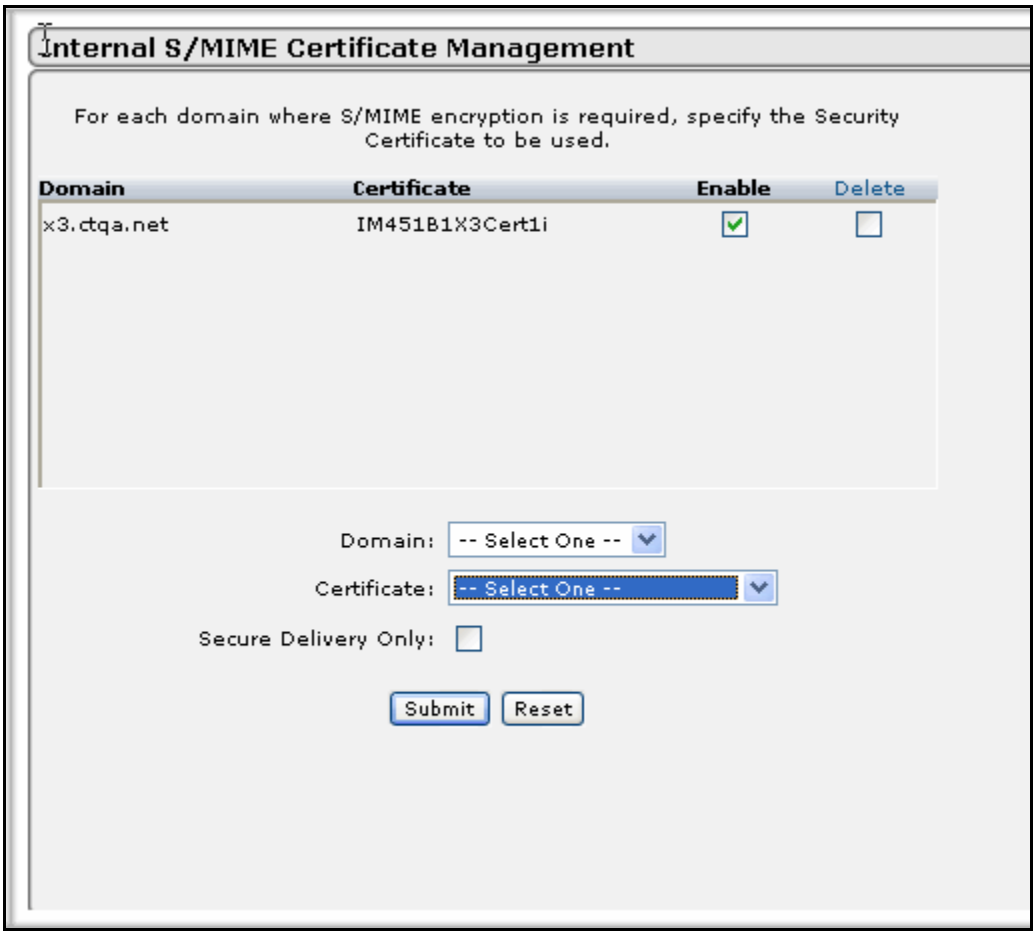
Field	Description
Domain	This column identifies the domains for which S/MIME encryption is required.
Cert Information	This column identifies the name of the S/MIME public key Security Certificate selected for use with the specified domain.
Enable	The **Enable** check box is selected by default when a domain is added to this table. When selected, IronMail will always attempt to send messages to this domain using S/MIME. When disabled, IronMail will attempt deliver messages using any other Secure Delivery mechanisms.
Secure Mode	Select the **Secure Mode** check box to force IronMail to send the messages securely or not at all. When selected and IronMail is unable to deliver the message using S/MIME, it will attempt to deliver it securely with any of IronMail's other Secure Delivery mechanisms. If it cannot, IronMail will not deliver the message. If Quarantine Undeliverable Messages is enabled in SMTPO Properties, IronMail will quarantine it to the *Failure Quarantine Queue*.
Delete	Select a domain's **Delete** check box to remove it from the table, and stop forcing S/MIME delivery to that domain.
Adding a New Domain	***The fields at the bottom of the screen permit adding a new domain.***
Domain	Enter the *domain name* for a new domain you wish to add to the list, to which IronMail should always send messages using S/MIME.
Secure Delivery Only	Select the **Secure Delivery Only** check box to require S/MIME encryption. When selected and IronMail is unable to deliver the message using S/MIME, it will attempt to deliver it securely with any of IronMail's other Secure Delivery mechanisms. If it cannot, IronMail will not deliver the message.
Certificate	Select from the pick list the proper certificate for the domain being added.

Enter any changes or new domains by clicking **Submit**. The screen will update.


External S/MIME Certificate Management
The data has been updated successfully!
For each domain where S/MIME encryption is required, specify the Security Certificate to be used. Add appropriate data for the certificates.
Enable S/MIME
Domain
Cert Information
Enable
Secure Mode
Delete
d11123.ctqa.net
d11123
dummy.com
x04
mydomain.org
IM45B61X3Cert1i
sm.ctqa.net
IM410B73SMCert1i_0913
Domain:
Secure Delivery Only:
Certificate:
-- Select One --
Submit
Reset

Internal S/MIME

The S/*MIME* page is used to specify internal domains hosted by IronMail that are required to receive messages securely using S/MIME. For each domain, specify which IronMail Security Certificate is to be used to provide the encryption.



The S/MIME Certificate Management table displays the following information:

Domain	This column displays the names of domains that are required to receive messages securely.
Certificate	This column displays the name of the Security Certificate IronMail will use to provide the encryption.
Enable	If enabled, IronMail will support S/MIME secure delivery when the sending server requests its use. If disabled, IronMail will not support S/MIME when sending servers request it.
Delete	Select domain's **Delete** check box and click **Submit** to remove it from this table. When a domain is removed from the S/MIME Certificate Management table, IronMail will no longer support S/MIME data encryption for messages addressed to that domain.
Adding a Domain	***The pick lists and check box at the bottom of the screen allow adding another domain to the list.***

Domain	The pick list is populated with any IronMail-hosted domains appearing in the *Mail-Firewall > Mail Configuration > Domain-based Routing table*. Select a domain. The domain will be added to the table, and IronMail will support S/MIME encryption when sending servers request it.
Certificate	The pick list is populated with the names of the Security Certificates installed on IronMail. (These Security Certificates were installed in *System > Certificate Manager*.) Select a Security Certificate that IronMail should use to encrypt messages addressed to the specified internal domain.
Secure Delivery Only	Click the check box to indicate this domain can only receive messages using S/MIME.

Click **Submit** to save all changes and additions.

PGP

IronMail provides the ability to send and receive server-based messages with PGP encryption, using much the same functionality as Mail-VPN.

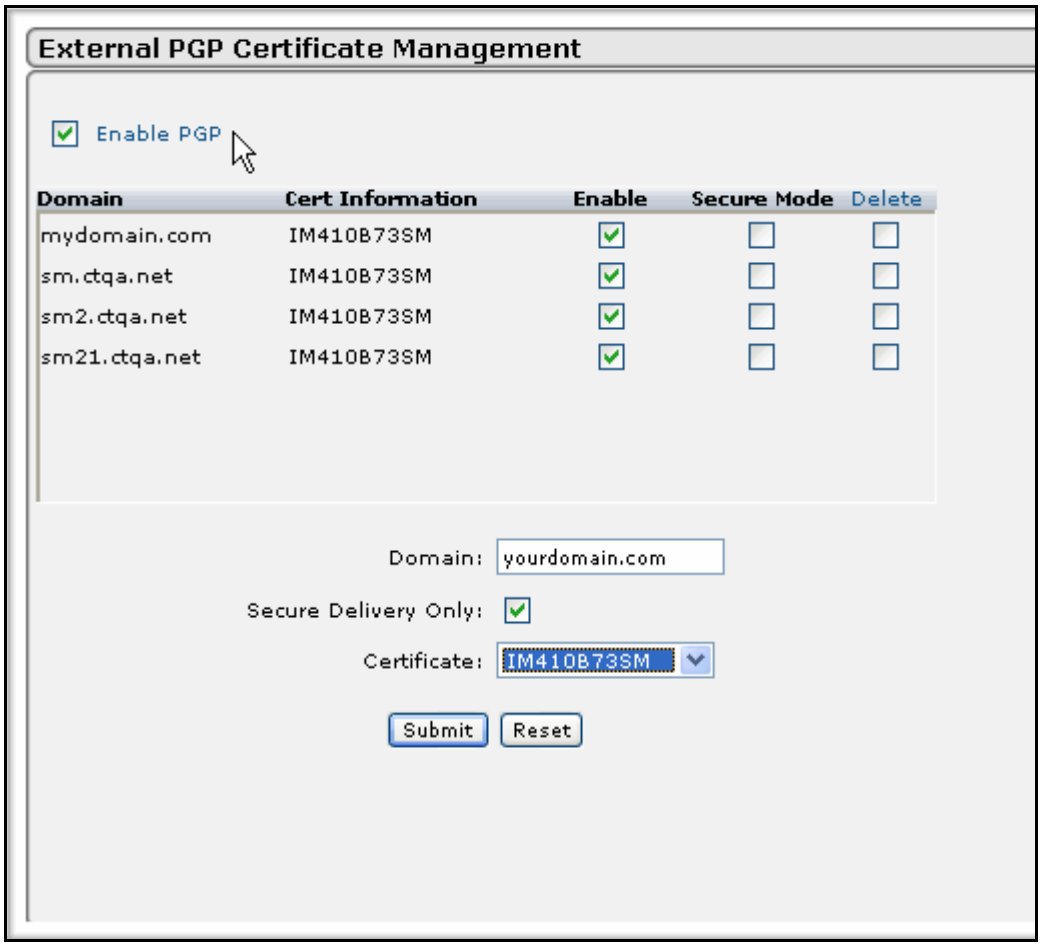
Every incoming message is checked to see if it is a PGP message. If so, IronMail checks to see if a key exists to decrypt the message. If a key exists, IronMail decrypts the message. If no key exists, the message is flows, providing that *Policy* Manager has not been configured to block PGP messages to the specific user.

Outgoing messages are checked for a domain or user that exists in the PGP encryption list. Different keys are required for different domains.

External PGP Key

Use this PGP page to manage the specific domains to which IronMail should send messages using PGP encryption.

Select the **Enable PGP** check box to instruct IronMail to require PGP encryption when sending messages to domains listed in the PGP table of domains. (IronMail sends PGP outbound messages in RFC3156-compliant format—i.e. signed and encrypted.)

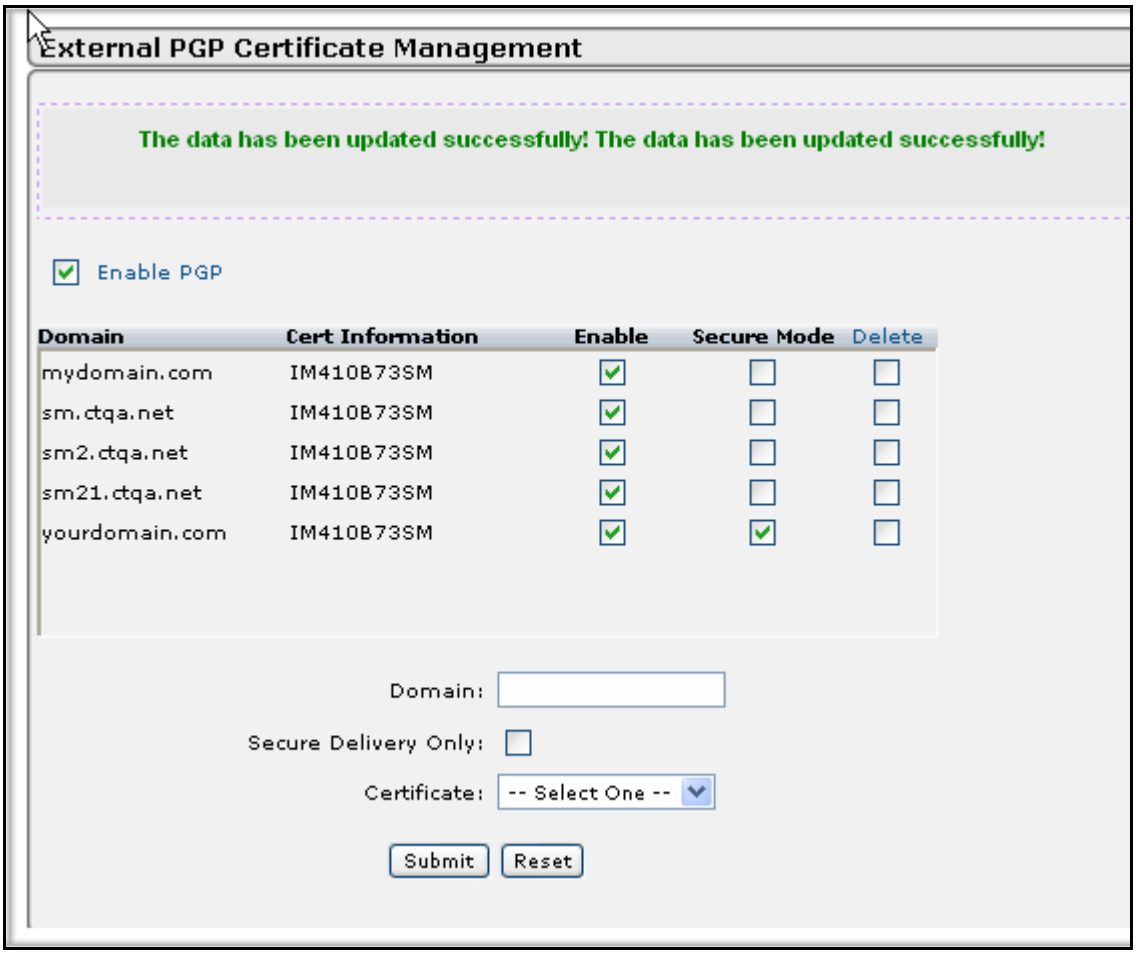


The table of PGP domains is populated by the domains whose Security Certificates have been installed on IronMail in *Secure Delivery > PGP Key Manager > Import*. The table provides information and requests the following user input:

Domain	This column identifies the domains for which PGP encryption is required. (Domains appear in this table only when PGP Security Certificates for them were installed in *Secure Delivery > PGP Key Manager*.)
Cert Information	This column lists the names of the certificates associated with each domain.
Enable	The **Enable** check box is selected by default when a domain is added to this table. When selected, IronMail will always attempt to send messages to this domain using PGP. To temporarily remove the requirement of encrypting messages to the specified domain without removing the domain from the table, deselect this option. When deselected, messages to that domain will be delivered in plain text.
Secure Mode	Select the **Secure Mode** check box to force IronMail to send the messages securely or not at all. When selected and IronMail is unable to deliver the message using PGP, it will attempt to deliver it securely with any of IronMail's other secure delivery mechanisms. If it cannot, IronMail will not deliver the message. If Quarantine Undeliverable Messages is enabled in SMTPO Properties, IronMail will quarantine it to the *Failure Quarantine Queue*.
Delete	Select a domain's **Delete** check box to remove it from the table, and stop forcing PGP delivery to that domain.

Adding a New Domain	***The lower portion of the screen contains data fields that may be used to add a domain to the list.***
Domain	Enter the *domain name* for the domain you wish to add.
Secure Delivery Only	Check the check box to indicate that IronMail will only send messages to this domain using PGP encryption.
Certificate	Select the proper certificate from the pick list.

Click **Submit** to save user input. The screen refreshes.



Internal PGP

The PGP Key Management table displays any internal domain for which a PGP Security Certificate was installed on IronMail. (PGP Security Certificates are installed either at *Secure Delivery > PGP Key Manager > Generate* or *Secure Delivery > PGP Key Manager > Import*.)

Administrators may enable/disable use of PGP encryption, or permanently remove the use of PGP for a domain.

IronMail only supports incoming PGP messages that are *RFC3156-compliant.*

The PGP Key Management table displays the following information:

Field	Description
Domain	This column displays the names of domains for which a PGP Security Certificate has been installed on IronMail. (Administrators installed and "mapped" a key to an internal domain at (*Secure Delivery > PGP Key Manager > Generate* or *Secure Delivery > PGP Key Manager > Import*.)
Cert Information	This column lists the names of the certificates associated with the internal domains that use or require PGP encryption.
Enable	If Enabled, IronMail will support PGP secure delivery when the sending server requests its use. If disabled, IronMail will not support PGP when sending servers request it.
Delete	Select domain's **Delete** check box and click **Submit** to remove it from this table. When a domain is removed from the PGP Key Management table, IronMail will no longer support PGP data encryption for messages addressed to that domain.
Adding a Domain	***The fields in the lower portion of the screen allow adding domains to the table.***
Domain	The pick list is populated with any IronMail-hosted domains appearing in the *Mail-Firewall > Mail Configuration > Domain-based Routing table*. Select a domain. When the domain is added to the table, IronMail will support PGP encryption when sending servers request it.

Certificate	The pick list is populated with the names of the Security Certificates installed on IronMail. Select a Security Certificate that IronMail should use to encrypt messages addressed to the specified internal domain.
Secure Delivery Only	Click the check box to indicate this domain can only receive messages using PGP encryption.

Click **Submit** to save the user input.

Secure Web Delivery

SWD Overview

The use of outbound S/*MIME*, PGP, and TLS secure message delivery is contingent upon the ability of the receiving mail server to support these methods of encryption. If the receiving server does not have a suitable Security Certificate, or cannot accommodate a secure method for any reason, and IronMail's **Secure Mode** is enabled, IronMail will drop the message. Secure Web Delivery, then, is designed to provide a secure alternative to recipient-server encryption. IronMail can be configured to deliver the original message securely to the Secure Web Delivery Server, and create a new email to the original recipient that contains a hyperlink to the Secure Web Delivery appliance. The original recipient is invited to "click here" to read the message waiting for them. When the recipient opens a browser to retrieve the message, a Security Certificate installed on the Secure Web Delivery appliance forces an HTTPS session for the user, ensuring that the message is read in an encrypted session.

There are two ways of enabling the policies for a message's delivery using Secure Web Delivery:

1. If one of IronMail's Mail Monitoring policies requires Secure Delivery as a *policy* action, IronMail will use Secure Web Delivery as the "fall back" position. When "Secure Delivery" is the designated action, IronMail will attempt to deliver the message in the following order of encryption methods: S/MIME, PGP, and TLS. If it is unsuccessful delivering the message using these methods, IronMail will fall back to Secure Web Delivery.
2. Users and domains appearing in the *Secure Delivery > Secure Web Delivery > User List* table will always receive messages via HTTPS. Before IronMail's SMTPO Service delivers any message off the appliance, it will look for the address/domain in its User List. If the address or domain exists on the list, the SMTPO Service will redirect the message to the Secure Web Delivery Server, which will then generate a new email to the user indicating that a message is waiting to be read securely. (The email contains a URL pointing back to the original message now stored on the Secure Web Delivery Server.)

Secure Web Delivery is a licensable feature. If a Secure Web Delivery license is installed *after* IronMail's initial installation, the administrator must log out of the Web Administration user interface and log back in again before the Secure Web Delivery feature is displayed and functional.

When Secure Web Delivery is hosted on a Secure Web Delivery Server (separate from the IronMail appliance), it must be configured on both the IronMail and the Secure Web Delivery Server.

Secure Web Delivery requires that messages have a valid MIME. For messages that the IronMail RIPQ is unable to parse ("rip" the message into its constituent MIME parts) successfully, the Secure Web Delivery option is not available. When the SMTPO process checks for the availability of Secure Web Delivery, it also checks for the validity of the message for MIME.

Recipients of messages delivered via Secure Web Delivery have the ability to send secure replies or acknowledgements for those received messages. IronMail supports secure replies only to the

original senders over *SSL*. You may edit the subject of the message and configure the relay target. See Configure Secure Web Delivery for configuration details.

Configure Router

Configuration of Secure Web Delivery must be made on both the IronMail appliance and the Secure Web Delivery Server. This page describes configuration of Secure Web Delivery on the IronMail appliance.

Configure Secure Web Delivery Router
Select options below for configuring Secure Web Delivery. If a Secure Web Delivery Server license is installed on IronMail, IronMail's host name and IP address must be provided. (Also, select a Security Certificate from the pick list to be used to secure the Web Delivery.) If a Secure Web Delivery Redirector license is installed on IronMail, only enter the IP address of the server hosting the Web Delivery.
Enable Secure Web Delivery Router
Secure Web Delivery Router IP Address
10.50.1.130
Submit
Reset

The *IP address* of the Secure Web Delivery Server must be provided. IronMail will deliver the original message securely to the Secure Web Delivery Server at this address. The following user input is required:

Enable Secure Web Delivery	Select the **Enable Secure Web Delivery** check box to "turn on" this feature in IronMail.
IP Address	Enter the IP address of the Secure Web Delivery Server.

Click **Submit** to save the user input.

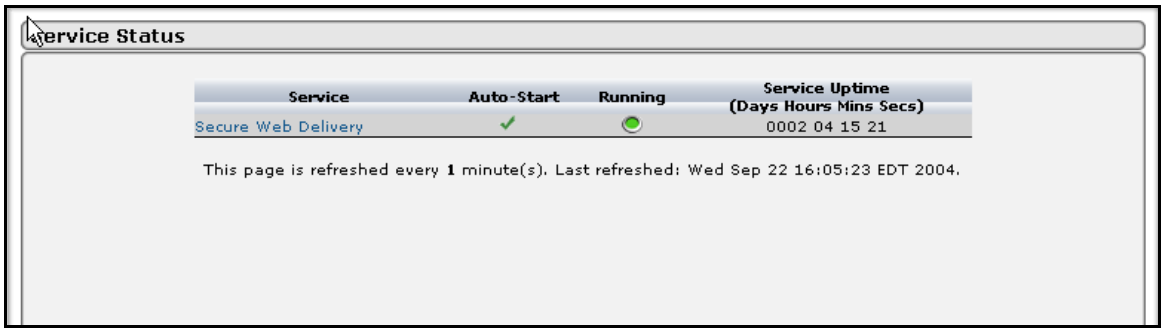
IronMail's IP address must be added to the Allow Relay list on the Secure Web Delivery Server.

Secure Web Delivery Server

The Secure Web Delivery (SWD) Server requires configuration on two pages: Configure Secure Web Delivery and Configure Server.

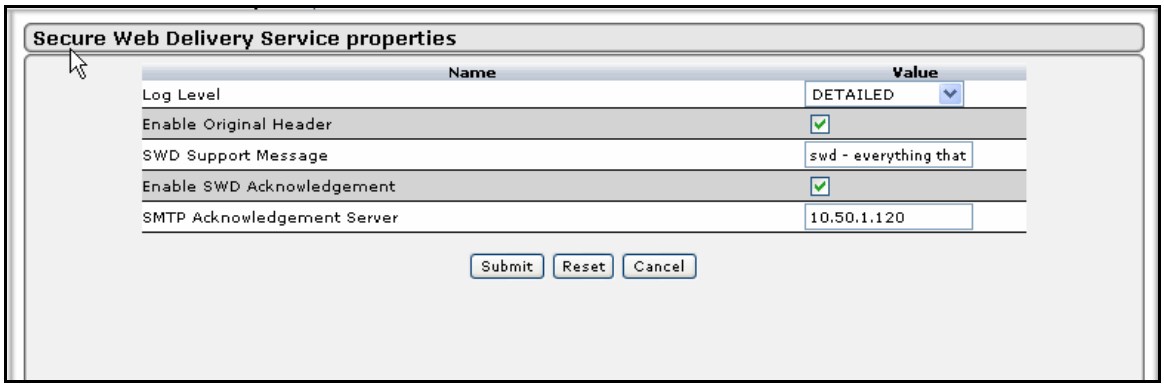
Configure Secure Web Delivery

The Configure Secure Web Delivery page starts and stops this Service, and allows configuration of the Service's properties.


Service Status
Service
Auto-Start
Running
Service Uptime (Days Hours Mins Secs)
Secure Web Delivery
0002 04 15 21
This page is refreshed every 1 minute(s). Last refreshed: Wed Sep 22 16:05:23 EDT 2004.

Service	The Service name (Secure Web Deliver) is a hyperlink that opens a secondary browser window allowing configuration of the Service's properties.
Auto-Start	A red X or green check icon indicates whether or not the Service is set to start automatically when the IronMail appliance is rebooted. If an icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green IronMail's Health Monitor will restart a Service that has stopped for any reason when it performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off. A service cannot start running, however, until its auto-start setting is turned on.) The red and green light icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from red to green. If the icon does not toggle as expected, click the **Configure Mail Services** hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped by an administrator or by an unexpected program error, but was restarted automatically by IronMail's Health Monitor.

When the Adminstrator clicks the Secure Web Delivery hyperlink, a secondary window opens, displaying five configurable properties:

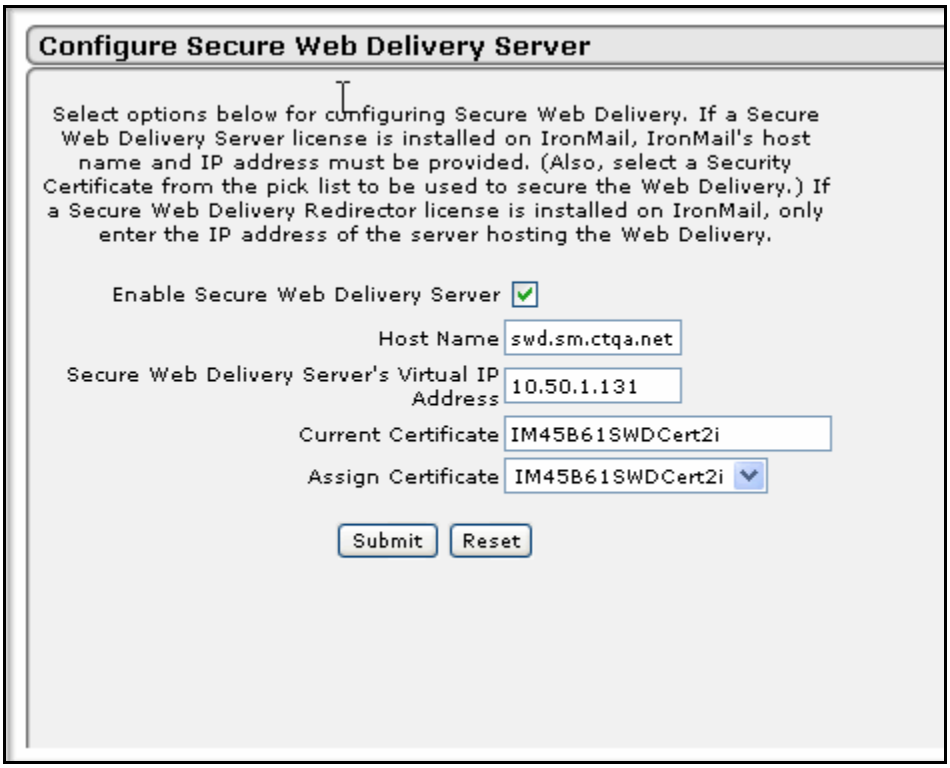


Log Level	Enter a logging level, indicating the amount of detail IronMail should include when logging Secure Web Delivery's message-processing. Options are: • Critical • Error • Information • Detailed
Enable Original Header	Select **Enable Original Header** to include all the RFC822 header information in the email notification the SWD Server presents to the end user. (This is the same header information that is viewed in the Message Details window when viewing messages from within one of IronMail's queues.) If this option is not enabled, the end user will only see the message's Date, Subject, and From address.
SWD Support Message	The SWD Server will insert the text string provided in this input field as the body of the message it will deliver to the end user, notifying him or her that a message is available for secure reading at the SWD-provided URL. An example of this text is: "A confidential message has been sent to you. You may read it securely through a browser by clicking the following URL." This URL is for adding any Help messages for the recipient (e.g., "contact 1-800-xxx-xxxx if you are not able to view the message").
Enable SWD Acknowledgement	Select this checkbox to enable SWD replies (acknowledgements) to the sender of the SWD message.
SMTP Acknowledgement Server	Enter the *IP address* of the SMTP server that will proxy the SWD secure replies. This IP address must also be included in the Allow Relay list for the Acknowledgement Server. If it is not on the Allow Relay list, an error message will display and the error will be logged in the ct_admin.log.

Click **Submit** to save the user input.

Configure Server

Administrators must create a virtual *IP address* and virtual *Host Name* for the Secure Web Delivery Server. (The virtual hostname must resolve in DNS to the *firewall*, router, or other *network* device that is "listening" for the virtual, or internal, IP address of the Secure Web Delivery Server.) End users, when reading/retrieving their email, will point their browsers to the virtual host name.


Configure Secure Web Delivery Server
Select options below for configuring Secure Web Delivery. If a Secure Web Delivery Server license is installed on IronMail, IronMail's host name and IP address must be provided. (Also, select a Security Certificate from the pick list to be used to secure the Web Delivery.) If a Secure Web Delivery Redirector license is installed on IronMail, only enter the IP address of the server hosting the Web Delivery.
Enable Secure Web Delivery Server
Host Name
swd.sm.ctqa.net
Secure Web Delivery Server's Virtual IP Address
10.50.1.131
Current Certificate
IM45B61SWDCert2i
Assign Certificate
IM45B61SWDCert2i
Submit
Reset

Enable Secure Web Delivery Server	Select the **Enable** check box to "turn on" the Secure Web Delivery functionality on the Secure Web Delivery appliance. If not enabled, IronMail will be unable to deliver messages via HTTPS for specified users, domains, or subjects of IronMail's email policies.
Host Name	Enter the hostname of the Secure Web Delivery (SWD) Server. This host name must resolve, in DNS, to the IP address of the firewall, router, or other network device that is listening for the virtual IP address of the SWD Server.
Secure Web Delivery's Virtual IP Address	Enter the virtual IP address of the SWD Server.
Current Certificate	The name of the currently-selected Security Certificate used to provide HTTPS security is identified. (*DEFAULT* refers to the unsigned certificate that is installed on IronMail by default in order to provide immediate HTTPS encryption of the Web Administration management sessions.)
Assign Certificate	All installed X.509 (S/*MIME* and *SSL*) Security Certificates will be displayed. Any one may be used.

Click **Submit** to save the user input.

User List

The User List page displays on both the IronMail appliance (*Secure Delivery > Secure Web Delivery > User List*) as well as on the Secure Web Delivery Server (*Secure Delivery > Secure Web Delivery > User List*). The User List on each appliance serve somewhat different purposes.

On the IronMail Appliance:

Users or domains appearing on IronMail's User List will *always* have messages delivered to them via Secure Web Delivery. Before IronMail delivers a message, it will first look in this list to

determine if it should be delivered normally or sent to the Secure Web Delivery server. If the domain or email address exists on the list, IronMail sends the message to the Secure Web Delivery Server which is responsible for generating a new email to the user that a message is waiting to be read securely. (The first time a message is delivered to a user on the User List, the Secure Web Delivery Server adds the account to its own User List.)

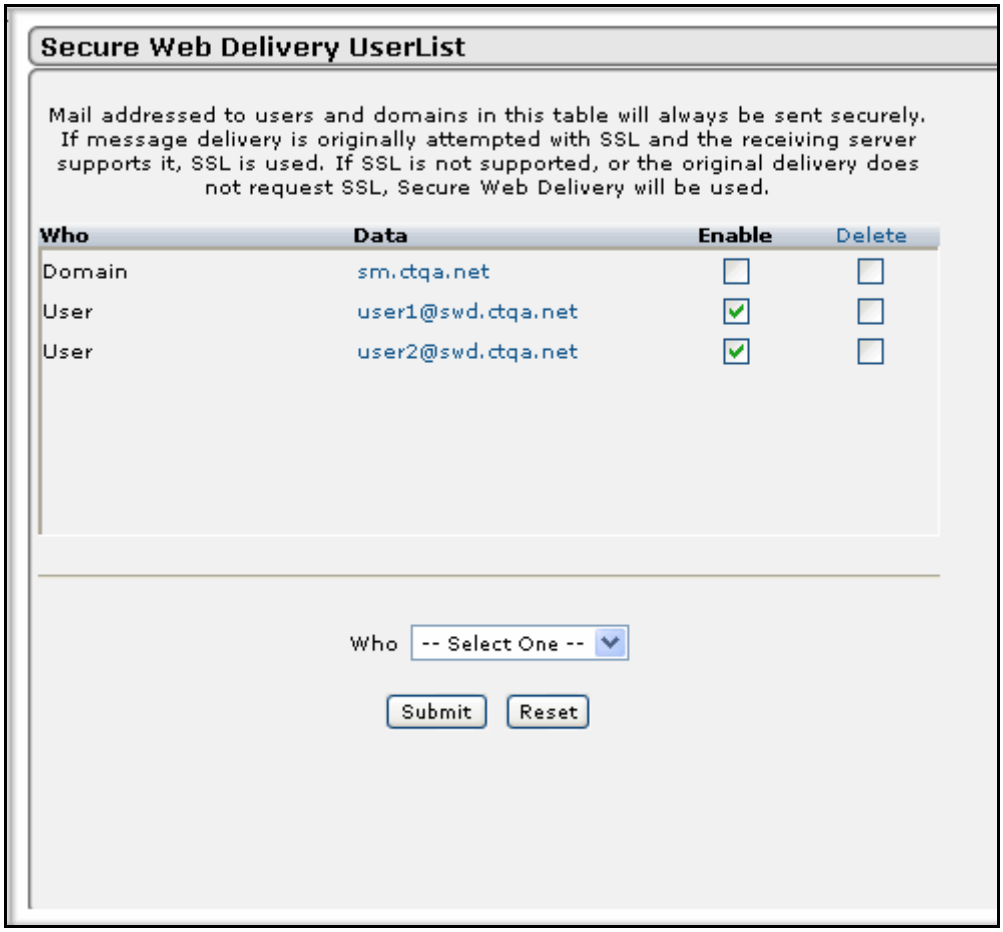
If an IronMail *policy* (e.g., a Mail Monitoring or Content Filtering policy) requires a Secure Delivery action, IronMail will first attempt to deliver the message via S/*MIME*, then PGP, and then *SSL*. If it cannot deliver the message via those methods, IronMail will fall back to Secure Web Delivery. When a message is delivered by Secure Web Delivery because of an IronMail policy, the user *is not added* to the User List on the IronMail.

On the Secure Web Delivery Server:

The purpose of the User List on the Secure Web Delivery Server is to manage passwords and logons. Administrators can create and delete passwords, as well as reset the "failed logon" count back to zero. If a user or domain is deleted from this User List but not deleted from IronMail's User List, it will be recreated the next time a message is addressed to that user/domain. (To permanently stop Secure Web Delivery for a user/domain, disable or delete the account from IronMail's User List.)

The User List Screen

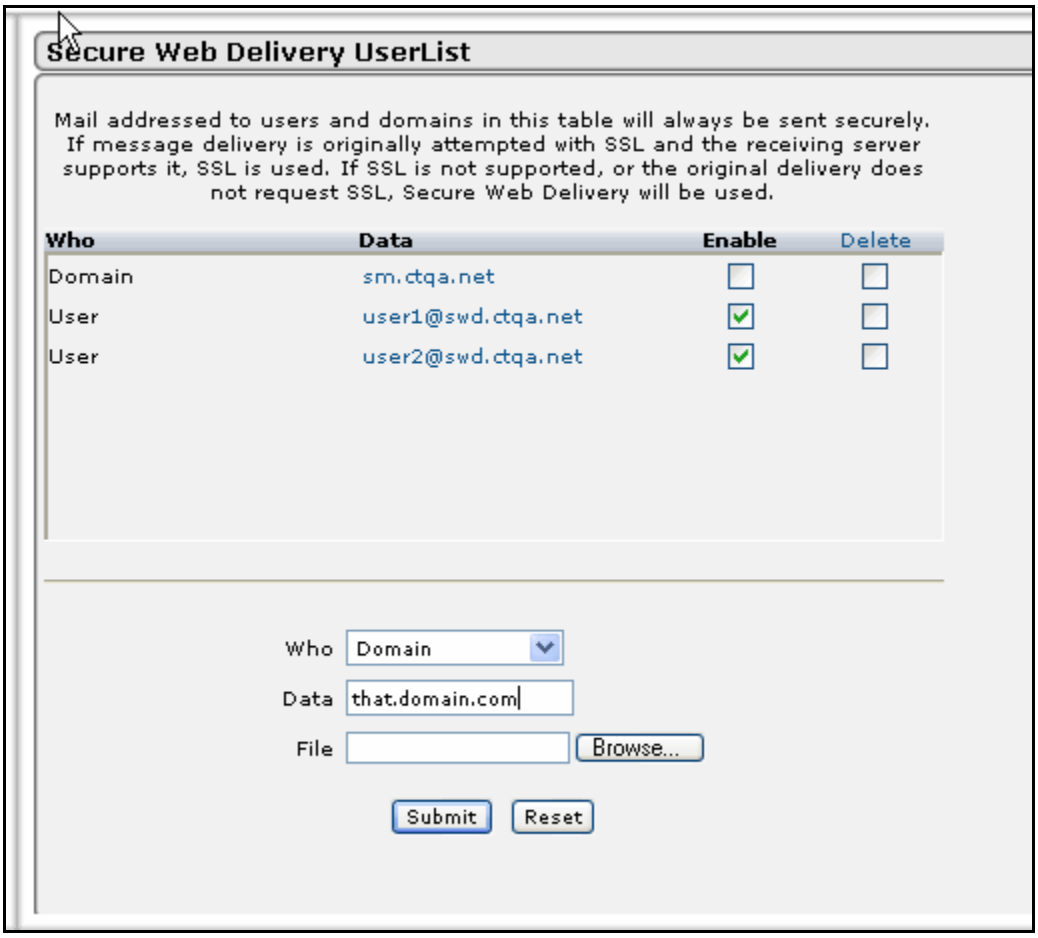
The Secure Web Delivery User List displays users or domains, as shown below.


Secure Web Delivery UserList
Mail addressed to users and domains in this table will always be sent securely. If message delivery is originally attempted with SSL and the receiving server supports it, SSL is used. If SSL is not supported, or the original delivery does not request SSL, Secure Web Delivery will be used.
Who
Data
Enable
Delete
Domain
sm.ctqa.net
User
user1@swd.ctqa.net
User
user2@swd.ctqa.net
Who
-- Select One --
Submit
Reset

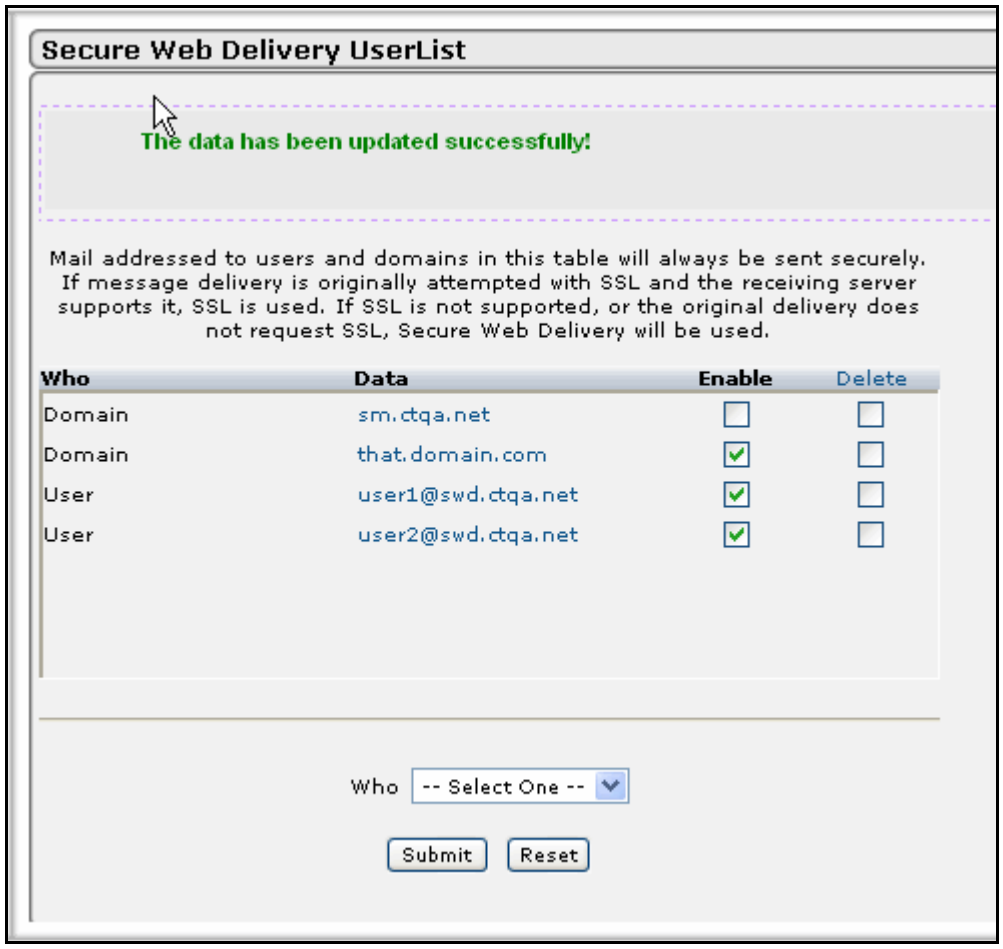
The Secure Web Delivery User List table displays the following information:

Who	This column displays whether an individual user or domain is indicated. (Secure Web Delivery will be enforced for the individual user or all the users within the domain.)
Data	This column displays the name of the user or domain.
Enable	The **Enable** check box "turns on" Secure Web Delivery for an individual or domain. (When selected, Secure Web Delivery will always be used as the delivery mechanism for the individual user or all users within the domain.) If **Enable** is deselected, IronMail will not deliver the message via Secure Web Delivery. (User accounts and domains may appear on the User List without being enabled or "active.")
Delete	The **Delete** check box allows the IronMail administrator to delete a user or domain from the User List table. Select the **Delete** check box for a user or domain and click **Submit**.

Add a new user to the list by selecting "User" or "Domain" from the **Who** pick list. The necessary entry fields display.

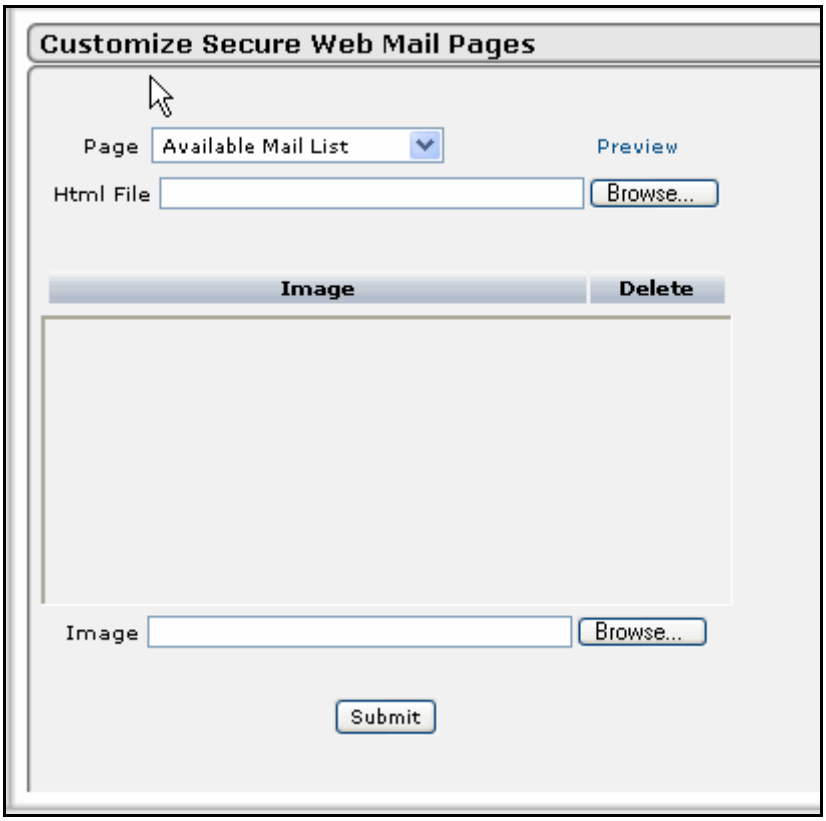


Enter or browse to the domain you wish to add, then click **Submit**. The screen refreshes.


Secure Web Delivery UserList
The data has been updated successfully!
Mail addressed to users and domains in this table will always be sent securely. If message delivery is originally attempted with SSL and the receiving server supports it, SSL is used. If SSL is not supported, or the original delivery does not request SSL, Secure Web Delivery will be used.
Who
Data
Enable
Delete
Domain
sm.ctqa.net
Domain
that.domain.com
User
user1@swd.ctqa.net
User
user2@swd.ctqa.net
Who
-- Select One --
Submit
Reset

Customizing SWD Pages

Specific SWD pages may be customized to promote the enterprise's company identity. More detailed information about customizing screens may be found in the Customizing Pages chapter of this manual.



The image below shows the default configuration of the Available Mail List page.

Note: The Secure Web Delivery customization feature is found only on dedicated SWD IronMail appliances. It is not available on regular IronMails.

Checking Logs

Under normal circumstances, you will not be able to tell if a message is transmitted securely. The only way to be sure a message was sent securely from gateway to gateway is to look at the logs on the IronMail appliance. The logs to view are the SMTPO log and the JOINQ log. Examples are shown below.

From the JOINQ log:

QSpinner:43415-04192004 13:16:56::No. of messages in qList: 1
QSpinner:43415-04192004 13:16:56::Creating Channel Object for message <53501>
QSpinner:43415-04192004 13:16:56::Starting Channel Thread for message <53501>
JOINQ:04192004 13:16:56:Ending Spin Run #43415
JOINQ:04192004 13:16:56:Sleeping Run #43416
43415:2:1:04192004 13:16:56:Message ID : <53501>
43415:2:1:04192004 13:16:56:Joining the part for the message <53501>
43415:2:1:04192004 13:16:56:Stage 1 starting: fn=</ct/data/mss/00/00/00/53/501>
43415:2:1:04192004 13:16:56:Secure status ::: S/*MIME* PGP SWMR SWMS
43415:2:1:04192004 13:16:56:**Secure domains ::: S/MIME <['billclintonsbook.com']> PGP <['billclintonsbook.com']> SWMR <[]> TLS <[]>**
QSpinner:43415-04192004 13:16:56::Completed Starting Channel Thread for message <53501>
QSpinner:43415-04192004 13:16:56::Waiting Round of 2 threads
QSpinner:43415-04192004 13:16:56::Ending Spinner thread.
43415:2:1:04192004 13:16:56:Secure failures::: S/MIME <[]> PGP <[]>
43415:2:1:04192004 13:16:56:Delivery Modes: <{'billclintonsbook.com': 2}>
43415:2:1:04192004 13:16:56:Encrypt action list: <{}>
43415:2:1:04192004 13:16:56:Delivery Modes: <{'billclintonsbook.com': 2}> SWM Domains <[]>
43415:2:1:04192004 13:16:56:Channel thread Ended for message <53501>

From the SMTPO log:

QSpinner:43414-04192004 13:16:57::QLIST RECEIVED [Domain: billclintonsbook.com, Delv-Mode: 2, MsgIds: [53501]]
43414:1:0:04192004 13:16:57:Starting to process for domain <billclintonsbook.com> and msgids <[53501]>
43414:1:0:04192004 13:16:57:Processing billclintonsbook.com
QSpinner:43414-04192004 13:16:57::Waiting Round of 1 threads
QSpinner:43414-04192004 13:16:57::Completed spinning channels.
43414:1:0:04192004 13:16:57:Lookup Returned. Data = <(10, 'billclintonsbook.com')>, Type = <MX>
43414:1:0:04192004 13:16:57:Lookup Returned <[(10, 'billclintonsbook.com', ('68.193.236.134',))]>.
43414:1:0:04192004 13:16:57:Connecting to Domain billclintonsbook.com
43414:1:0:04192004 13:16:57:Block time out set to = (300) seconds.
43414:1:0:04192004 13:16:57:Connecting to MX <billclintonsbook.com> ....
43414:1:0:04192004 13:16:57:Connecting to A <68.193.236.134> ....
43414:1:0:04192004 13:16:57:Connection Status ------<1>
43414:1:0:04192004 13:16:57:**The messages for the domain <billclintonsbook.com> are S/MIME encrypted. Connection might get established non secured.**
43414:1:0:04192004 13:16:57:Recipient Server Certificate verification failed. Verification is not enabled. Continuing...
43414:1:0:04192004 13:16:57:Starting SendSmtpMsg for msg_id <53501> in domain <billclintonsbook.com>
43414:1:0:04192004 13:16:57:Sendmail Begin from : trent.greenwood@cannibalhockey.com

43414:1:0:04192004 13:16:58:**RETR COMMAND RECEIVED**
('/ct/data/mss/00/00/00/53/501.smime',)
43414:1:0:04192004
13:16:58:LOG_STAT|trent.greenwood@cannibalhockey.com|['herb@billclintonsbook.com']|1557|2
004/04/19 13:16:58|2
43414:1:0:04192004 13:16:58:Closing SMTP Connection
43414:1:0:04192004 13:16:58:Finished to process for domain <billclintonsbook.com> and
msgids <[53501]>

IRONMAIL ADMINISTRATION

Reporting and Monitoring

IronMail's reporting and monitoring tools are what make IronMail such a robust and usable appliance. Through its logs, administrators can determine exactly which IronMail processes examined a message—indeed, whether or not IronMail even received the message. When an IronMail *policy* acts upon a message, the reports and logs will describe exactly what condition of the policy caused IronMail to act.

In addition to reporting on IronMail's internal message-processing, this program area also contains "Health Monitor"—a subsystem that examines all other core application subsystems, as well as hardware, to ensure that the appliance is operating as designed. And on the belief that IronMail cannot truly protect an enterprise's email system if the appliance, itself, is vulnerable, an Alert Manager can be configured to generate email, pager, or SNMP trap alerts to the administrator whenever Health Monitor detects that IronMail is not performing as designed.

The first four hyperlinks in the left navigation frame of the Administration program area provide access to:

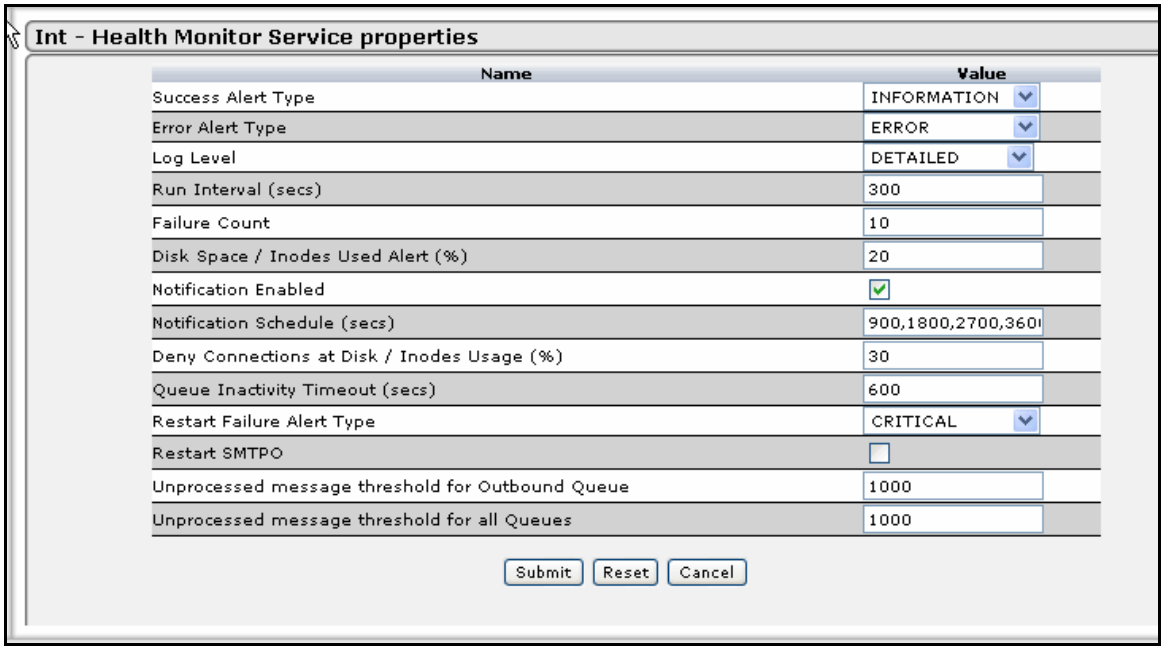
- Health Monitor: IronMail's subsystem that monitors other core, internal subsystems and hardware.
- DNS Hijack Protection: IronMail may be configured to verify that the enterprise DNS records for the mail servers it protects are correct—i.e. the DNS's MX and A records have not been "hijacked."
- Alert Manager: IronMail may be configured to send the alerts that it generates to administrators via email, pager, or SNMP traps.
- Reports/Log Files: IronMail's logs and daily reports provide remarkable visibility into every step of IronMail's message processing.

Health Monitor

Health Monitor is an IronMail subsystem that examines the appliance's overall performance, running a series of tests to ensure that all services and processes are performing as designed. Health Monitor "wakes up" at a user-defined interval and runs automatically in the background to test its many subsystems. IronMail will also monitor the status of any internal servers that are "in-line" with IronMail (Health Monitor will send the mail server a connection request to ensure that it is responsive).

Note: If an intermediary device is between IronMail and the mail server, Health Monitor will incorrectly infer from the intermediary device's response that the internal server is functioning normally.

Health Monitor options may be configured by clicking the Configure hyperlink on the page. The Int - Health Monitor Service Properties window opens displaying Health Monitor's configuration options.



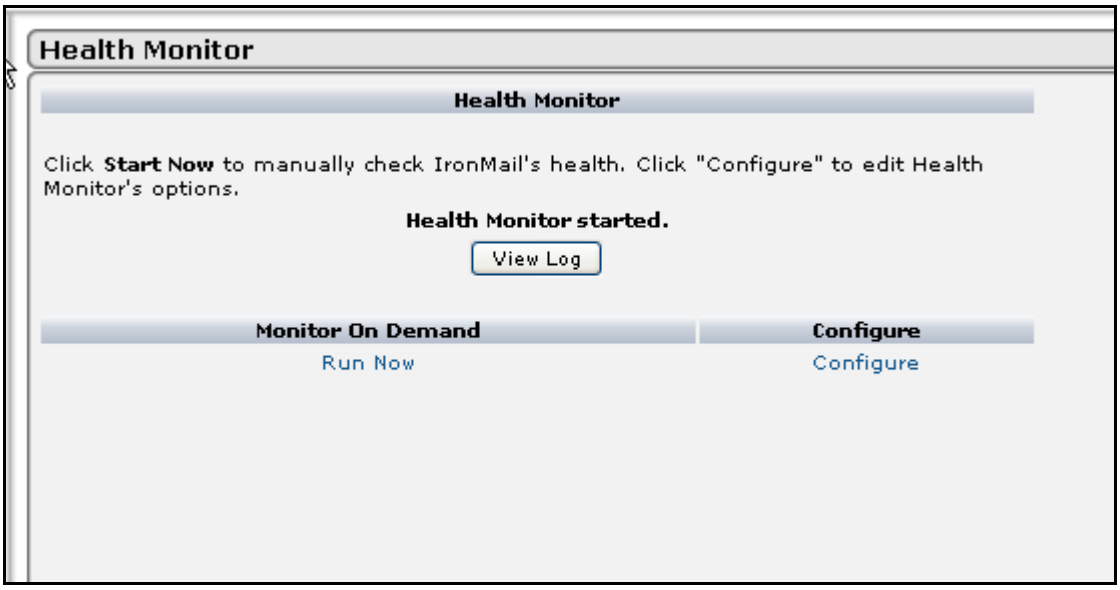
Field	Description
Success Alert Type	Select the Alert Type to be generated when Health Monitor runs successfully.
Error Alert Type	Select the Alert Type to be generated when Health Monitor encounters an error.
Log Level	IronMail offers 4 levels of logging, primarily to assist CipherTrust Support engineers when technical support is required. Select the log level you prefer. Options are: • Critical • Error • Information • Detailed View Health Monitor's log by navigating to *Monitoring > Reports/Log Files > Detailed Logs > "Int - Health Monitor."*

Run Interval (secs)	Enter a number representing, in seconds, the length of time from when the Health Monitor completes one run to when it starts another. It is recommended that this Run Interval not be set lower than the default 300 seconds (five minutes). During periods of high IronMail activity—e.g., heavy mail load—it may take several minutes or more for Health Monitor to finish its tests.
Failure Count	Enter a number representing how many times Health Monitor should repeat a failed system test before recording the failed test as an error. If this value is set to "10," and a certain test fails 9 times but passes on the 10th try, IronMail does not record an error. Only if the test fails on the 10th successive attempt will IronMail log it as a error and move on to the next test. It is highly recommended that this default value (10) not be changed without first consulting with CipherTrust Technical Support. If "Notification" is enabled below, and IronMail's Alert Manager is configured for it, IronMail will send an email, pager, or SNMP alert to the administrator when this occurs.
Disk Space/Inodes Used Alert (%)	While there is a small disk partition devoted to the appliance's operating system, all of IronMail's program files, email Message Store, and temporary files reside on one, separate partition. The number entered in this input field represents how "full" the partition may become before generating an alarm. If "Notification" is enabled below, and IronMail's Alert Manager is configured for it, IronMail will send an email, pager, or SNMP alert to the administrator when this threshold is reached. It is recommended that the default threshold (75%) be accepted in the beginning. After IronMail is fully "in-line" in the mail flow, and its logs and reports have accumulated on disk for several days, administrators can use IronMail's System Graphs to view actual disk utilization. IronMail's disk utilization may also be seen using the Command Line Interface.
Notification Enabled	If this option is enabled, Health Monitor will send alerts for any errors it detects to IronMail's Alert Manager. Though the Alert Manager may receive the alerts from the Health Monitor, the alerts are not delivered to the administrator unless the Alert Manager has been configured to do so. Health Monitor will send notifications in case of errors in the following areas: • SMTPI Service • SMTPIS Service • *POP3* Service • POP3S Service • *IMAP4* Service • IMAP4S Service • JSP interpreter (responsible for creating IronMail's Web Admin pages) • DNS Hijack Protection • Internal Queues (Rip and Join) • Web Administration (IronMail's browser interface) • Anti-Virus Queue • Mail Monitoring Queue • Content Filtering Queue • Anti-Spam Queue • Outbound Queue • Disk Space warning • Cryptoaccelerator Card (if present) • Internal Mail Servers • Reports • IronWebMail • Secure Web Mail Queue • *CMC* and Administration

	Connection • SSHD Client
Notification Schedule	Health Monitor runs its tests on core subsystems and hardware every user-defined number of seconds (see "Run Interval" above). Rather than repeatedly generating alerts every time it detects the same error in successive tests, it will only generate alerts according to this "notification schedule." After the fourth notification, Health Monitor will *continue* sending alerts (if the condition persists) every *nnn* minutes, where *nnn* is the interval between the third and fourth notification. (E.g., if the notification schedule is 1 minute, 20 minutes, 1 hour, and 4 hours, subsequent notifications will be sent thereafter every three hours.) Enter four values, separated by commas, representing the number of seconds Health Monitor should wait before sending the same alert to IronMail's Alert Manager if, on a successive test, the condition still exists. Values must integers, and entered in increasing order.
Deny Connections at Disk Usage (%)	Enter a value, from 1 to 90, representing the maximum percentage of disk space utilization after which IronMail will stop accepting new messages. IronMail's SMTPI Service will stop accepting new SMTP connection requests when this threshold is reached. This value must be higher than the "Disk Space Used: Alert" value above.
Queue Inactivity Time-out (secs)	During Health Monitor's many tests, it looks at the time stamp when a message entered one of IronMail's queues, then compares it to the current system time. Taking into account how many messages are in the queue and IronMail's current "message load," if a message has remained in a queue more seconds than the number entered in this input field, Health Monitor will assume that particular Queue Service experienced a program error, and will stop and restart the service. If a "Queue Inactivity Time-out" is set to "0" (with the expectation that email should be processed by the queues *immediately*), Health Monitor may inaccurately report in its Detailed Log that a problem has occurred. That is, if there exists a slow pipeline to the internal mail server and/or high email volume, Health Monitor will report queue inactivity errors even though messages might be processed and flowing as expected. Initially, it is recommended that administrators accept the default period of inactivity of ten minutes (600 seconds). If the IronMail is processing large amounts of messages in a high email volume environment, the number of seconds may be increased.
Restart Failure Alert Type	Select the Alert Type to be generated when Health Monitor's attempt to restart a sub-system fails.
Restart SMTPO	If Health Monitor is supposed to restart the Outbound Queue, click the checkbox.
Unprocessed Message Threshold for Outbound Queue	Enter a number of messages to serve as the threshold for the Outbound Queue. This integer represents the maximum number of unprocessed messages that should be in the queue. If the threshold is met or exceeded, Health Monitor will generate an Alert.
Unprocessed Message Threshold for all Queues	Enter a number of messages to serve as the threshold for all queues. This integer represents the maximum number of unprocessed messages that should be in any one of the other queues at any time. If the threshold is met or exceeded, Health Monitor generates an Alert.

Click **Submit** when the information has been entered correctly.

Health Monitor may be run between its scheduled cycle times by clicking the Run Now hyperlink. Note that in older versions of Internet Explorer, such as those earlier than IE Version 5.5, the hyperlink may not function. If Health Monitor is manually run, allow it several minutes to complete all its tests before clicking the View Log button to view the results.



Clicking the View Log button opens the log file for Health Monitor. Detailed results of its tests appear in the log, as indicated in the sample portion shown below.

```
Setting Name=<trust_rootcert> Value = </ct/conf/pubstore/trustroot.pem>
Setting Name=<encrypt_mode> Value = <1>
Setting Name=<attachedToCMC> Value = <0>
Setting Name=<run_interval> Value = <300>
Setting Name=<allow_upward_restore> Value = <0>
Setting Name=<restartFailureAlertType> Value = <CRITICAL>
Setting Name=<oob_enabled> Value = <0>
Setting Name=<route_subdomain> Value = <1>
Setting Name=<monitor_ip> Value = <localhost>
Setting Name=<MemoryKbLimit> Value = <50000>
Setting Name=<shm_spamcount> Value = <100>
Setting Name=<cfReadSize> Value = <4>
Setting Name=<keyfile> Value = </ct/conf/apache/ct_serverkey.ber>
WATCH:09222004 00:08:59:Base Class readAllTables()
Summary Logger = <<rotating-file logger: <open file '/ct/data/admin/log/summary.log', m
WATCH:09222004 00:08:59:Program Parameters:
    ** ConfigFailurecount: 10
    ** ConfigFile: /ct/conf/config
    ** CycleTime: 300
    ** DefaultCycleTime: None
    ** DefaultHost: im.na.ctqa.net
    ** DenyConnThreshold: 30
    ** DiskPctLimit: 20
    ** EnabledProcesses: ['ripq', 'pop3sproxy', 'httpd', 'sshd_maint', 'smtpproxy', 'ad
    ** Host: None
    ** MaxThreads: 100
    ** MemoryKbLimit: 50000
    ** MonitorHost: localhost
    ** MonitorPorts: {'avq': 30200, 'schedrrd': 30169, 'watch': 30140, 'ripq': 30230, '
    ** NotifyEnable: 1
    ** NotifyTimes: [120L, 240L, 360L, 480L]
    ** Retries: None
    ** RunOnce: 0
    ** SbinDir: /ct/sbin/
    ** ServerPortList: {'eusrquarantine': 22503L, 'smtpsproxy': 465L, 'admin': 22502L,
    ** SmtpoCycleTime: 10
    ** SmtpoTimeout: 600
    ** StartupDelay: 0
    ** StatDir: /ct/data/stat/
    ** TestFile: None
    ** Verbose: 0
    ** WantNotify: 1
    ** WantRestart: 1
```

Health Monitor Tests and Alerts

Health Monitor (also known as "Watch") routinely runs the following tests, which may result in Alerts:

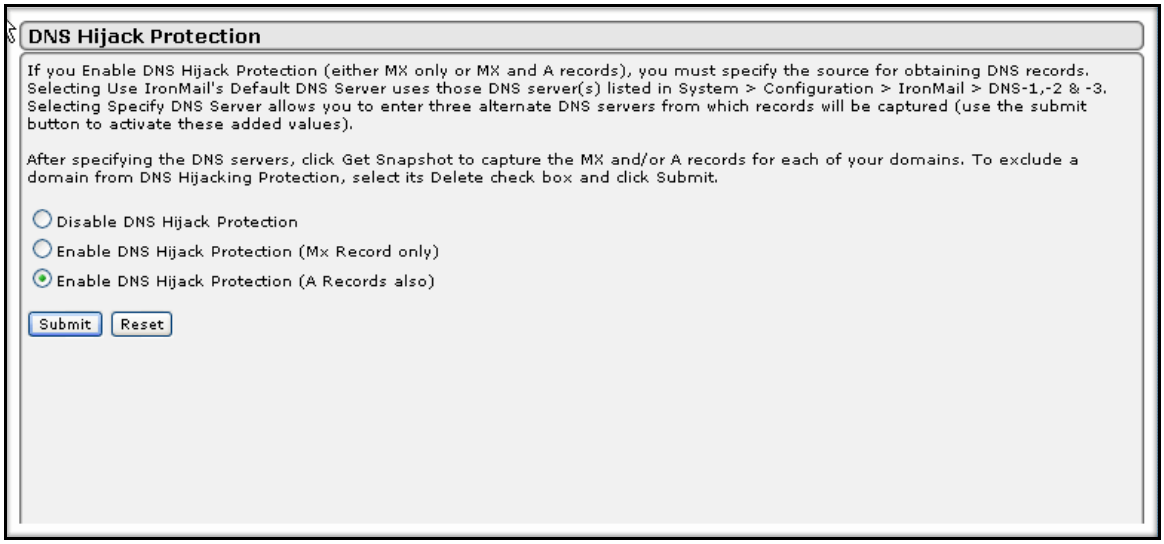
Test	Test Name
httpd	Web Administration Test
sys-crypto	System Status Test - Crypto
sys-disk	System Status Test - Disk
sys-inode	System Status Test - Inode
sshd_maint	SSHD Command Line Interface (CLI) Test
tomcat	Web Administration JSP Test
sys-cmcsql	System Status Test - *CMC* IronMail SQL Connection Test
sys-cmcadmin	System Status Test - CMC IronMail Admin Connection Test
reports	Reports Test
admin	Admin Server Test
spamq-count	Spam Queue Count Test
smtpo-count	SMTP Outbound Queue Count Test
superq-count	SuperQueue Count Test
vfq-count	Content Extraction Queue Count Test
ripq-count	Rip Queue Count Test
joinq-count	Join Queue Count Test
cfq-count	Content Filtering Queue Count Test
mmq-count	Mail Monitoring Queue Count Test
avq-count	Anti-Virus Queue Count Test
spamq	Spam Queue Test
mmq	Mail Monitoring Queue Test
avq	Anti-Virus Queue Test
cfq	Content Filtering Queue Test
joinq	Join Queue Test
ripq	Rip Queue Test
superq	SuperQueue Test
vfq	Content Extraction Queue Test
swmq	SWD Queue Test
smtpo	SMTP Outbound Queue Test
smtpproxy	SMTP Inbound Proxy Test

smtpsproxy	Secure SMTP Inbound Proxy Test
pop3proxy	*POP3* Proxy Test
pop3sproxy	Secure POP3 Proxy Test
imap4proxy	*IMAP4* Proxy Test
imap4sproxy	Secure IMAP4 Proxy Test
sys-dnshijack	System Status Test - DNS Hijack
iwm	Iron WebMail Test
swm-tomcat	SWM Web Admin JSP Test
urq-tomcat	URQ Web Admin JSP Test
eusrquarantine	EUQ Server Test

DNS Hijack Protection

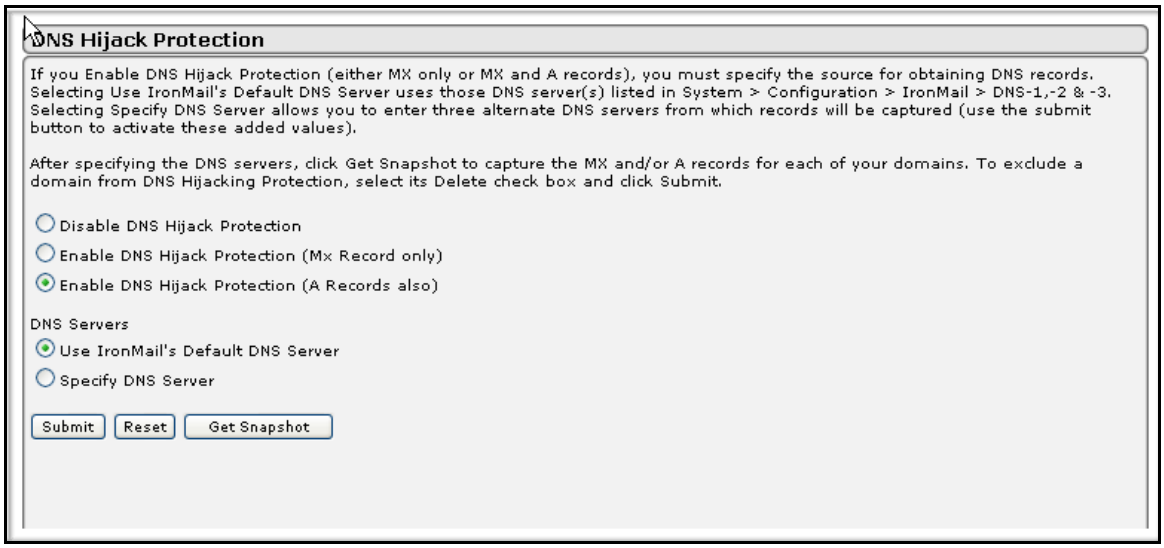
IronMail's daily, as well as "on demand," Program Integrity and Filesystem Integrity tests (*Mail-IDS > System Level*) ensure that administrators know in a timely fashion if hackers have added, deleted, or tampered with any files on the IronMail appliance. DNS Hijack Protection extends that protection to the enterprise *DNS server* by comparing the "known, good" MX and A record information on the DNS servers with the MX and A record information IronMail has cached locally on disk. If the MX or A records on the DNS server ever change from what IronMail expects them to be, the administrator is immediately notified. IronMail can perform this DNS query and comparison every time Health Monitor performs its tests.

The DNS Hijack Protection screen allows the Administrator to enable and configure the service.


DNS Hijack Protection
If you Enable DNS Hijack Protection (either MX only or MX and A records), you must specify the source for obtaining DNS records. Selecting Use IronMail's Default DNS Server uses those DNS server(s) listed in System > Configuration > IronMail > DNS-1,-2 & -3. Selecting Specify DNS Server allows you to enter three alternate DNS servers from which records will be captured (use the submit button to activate these added values).
After specifying the DNS servers, click Get Snapshot to capture the MX and/or A records for each of your domains. To exclude a domain from DNS Hijacking Protection, select its Delete check box and click Submit.
Disable DNS Hijack Protection
Enable DNS Hijack Protection (Mx Record only)
Enable DNS Hijack Protection (A Records also)
Submit
Reset

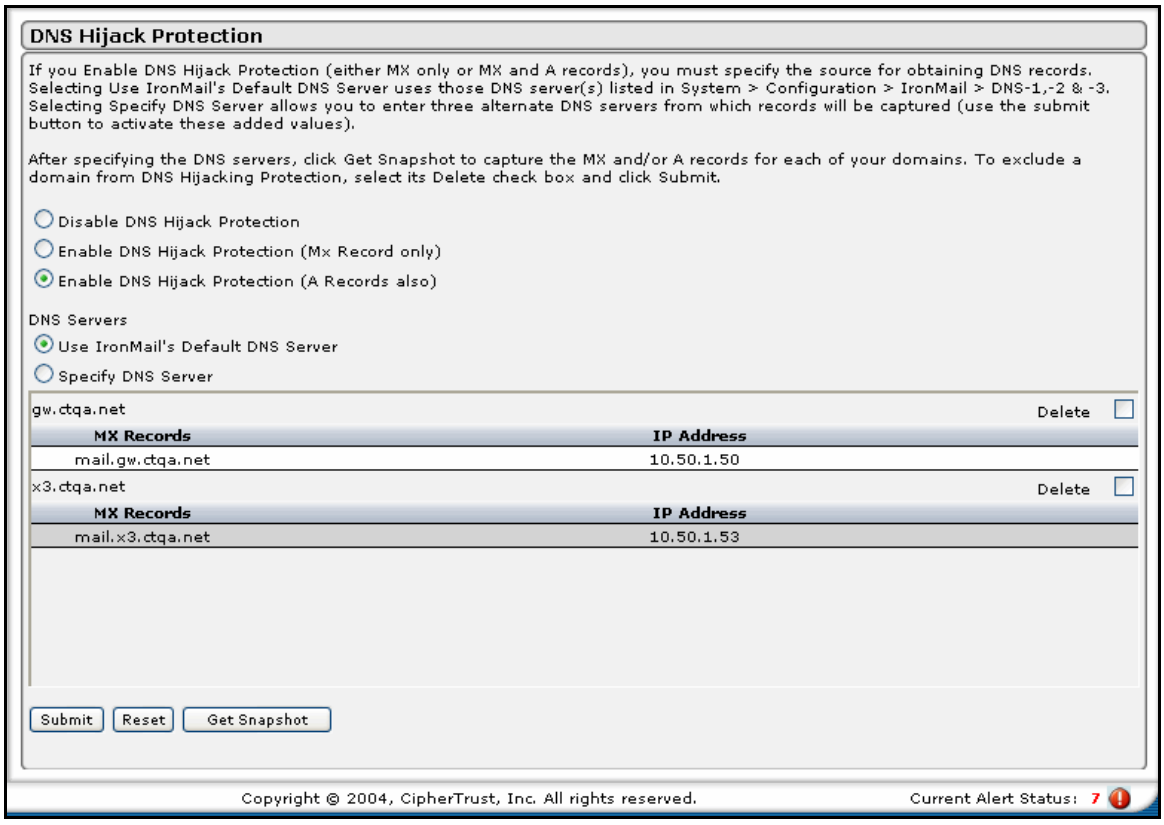
Configure	There are three configurations for DNS Hijack Protection: • **Disable DNS Hijack Protection:** When IronMail is initialized during initial installation, "DNS Hijack Protection" is disabled by default. However, since there is virtually no "performance overhead" to the system with it enabled, it is recommend that this be enabled. If the service is enabled, the Administrator must specify immediately below whether to obtain just the mail servers' MX records, or both MX and A records, and specify the DNS servers from whom it will get them. • **Enable DNS Hijack Protection (MX Record only):** This option will obtain and locally store the MX (mail exchange) record information for each mail server. (When selected, and after clicking **Submit**, **DNS Server** radio buttons and a **Get Snapshot** button appear immediately below.) • **Enable DNS Hijack Protection (A Records also)**: This option provides additional protection by storing and comparing both the MX and A records of the protected mail servers. (When selected, and after clicking **Submit**, **DNS Server** radio buttons and a **Get Snapshot** button appear immediately below.)

After making the selection, click **Submit**. Then specify the server preference to be configured.

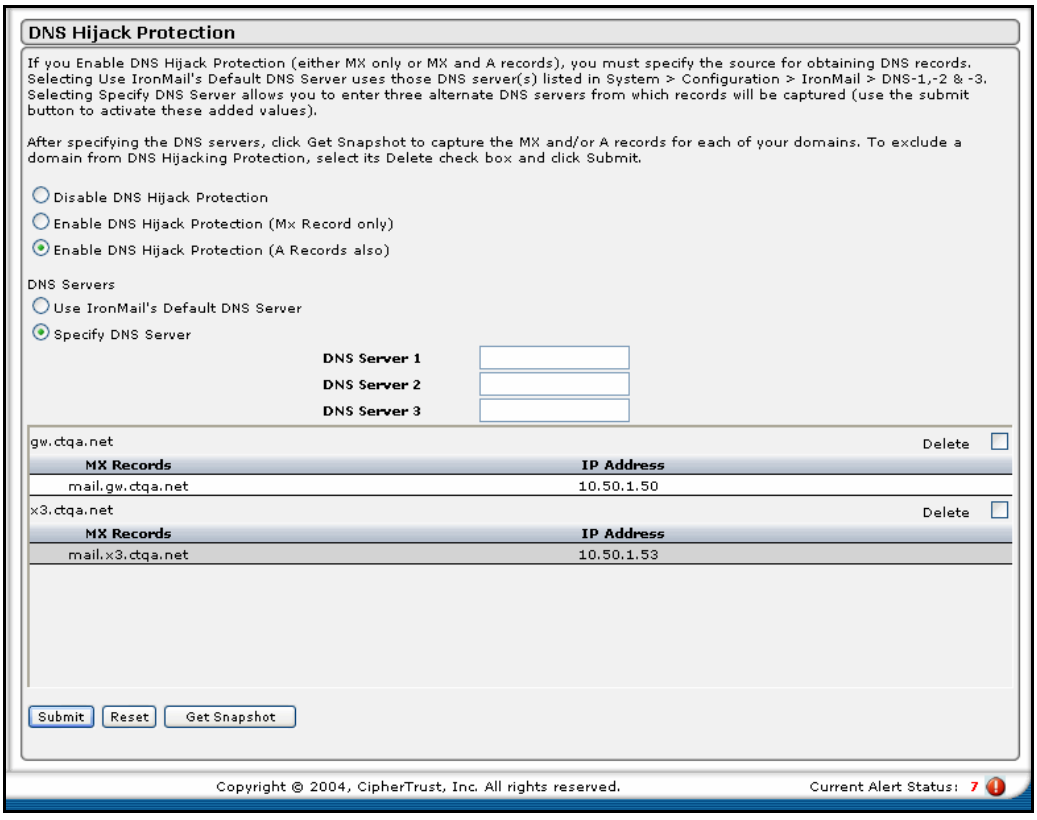

DNS Hijack Protection
If you Enable DNS Hijack Protection (either MX only or MX and A records), you must specify the source for obtaining DNS records. Selecting Use IronMail's Default DNS Server uses those DNS server(s) listed in System > Configuration > IronMail > DNS-1,-2 & -3. Selecting Specify DNS Server allows you to enter three alternate DNS servers from which records will be captured (use the submit button to activate these added values).
After specifying the DNS servers, click Get Snapshot to capture the MX and/or A records for each of your domains. To exclude a domain from DNS Hijacking Protection, select its Delete check box and click Submit.
Disable DNS Hijack Protection
Enable DNS Hijack Protection (Mx Record only)
Enable DNS Hijack Protection (A Records also)
DNS Servers
Use IronMail's Default DNS Server
Specify DNS Server
Submit
Reset
Get Snapshot

DNS Servers	• **Use IronMail's Default DNS Server:** Select this option to retrieve the MX/A records from the DNS server(s) identified in *System > Configuration > IronMail*. (The IP addresses of up to three DNS servers were provided during the Initial Configuration Wizard when IronMail was first installed. These are the "default" DNS servers.) • **Specify DNS Server:** Select this option to specify DNS servers other than those identified in *System > Configuration > IronMail*. When selected, three input fields are immediately displayed. Enter the IP addresses of up to three alternate DNS servers.

Click **Submit.** If the Administrator elects to use the default DNS server, the following screen appears.


DNS Hijack Protection
If you Enable DNS Hijack Protection (either MX only or MX and A records), you must specify the source for obtaining DNS records. Selecting Use IronMail's Default DNS Server uses those DNS server(s) listed in System > Configuration > IronMail > DNS-1,-2 & -3. Selecting Specify DNS Server allows you to enter three alternate DNS servers from which records will be captured (use the submit button to activate these added values).
After specifying the DNS servers, click Get Snapshot to capture the MX and/or A records for each of your domains. To exclude a domain from DNS Hijacking Protection, select its Delete check box and click Submit.
Disable DNS Hijack Protection
Enable DNS Hijack Protection (Mx Record only)
Enable DNS Hijack Protection (A Records also)
DNS Servers
Use IronMail's Default DNS Server
Specify DNS Server
gw.ctqa.net
Delete
MX Records
IP Address
mail.gw.ctqa.net
10.50.1.50
x3.ctqa.net
Delete
MX Records
IP Address
mail.x3.ctqa.net
10.50.1.53
Submit
Reset
Get Snapshot
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 7

If the Administrator selects Specify DNS Server, the screen appears as below.


DNS Hijack Protection
If you Enable DNS Hijack Protection (either MX only or MX and A records), you must specify the source for obtaining DNS records. Selecting Use IronMail's Default DNS Server uses those DNS server(s) listed in System > Configuration > IronMail > DNS-1,-2 & -3. Selecting Specify DNS Server allows you to enter three alternate DNS servers from which records will be captured (use the submit button to activate these added values).
After specifying the DNS servers, click Get Snapshot to capture the MX and/or A records for each of your domains. To exclude a domain from DNS Hijacking Protection, select its Delete check box and click Submit.
Disable DNS Hijack Protection
Enable DNS Hijack Protection (Mx Record only)
Enable DNS Hijack Protection (A Records also)
DNS Servers
Use IronMail's Default DNS Server
Specify DNS Server
DNS Server 1
DNS Server 2
DNS Server 3
gw.ctqa.net
Delete
MX Records
IP Address
mail.gw.ctqa.net
10.50.1.50
x3.ctqa.net
Delete
MX Records
IP Address
mail.x3.ctqa.net
10.50.1.53
Submit
Reset
Get Snapshot
Copyright © 2004, CipherTrust, Inc. All rights reserved.
Current Alert Status: 7

After DNS Hijack Protection is enabled, a "snapshot" of the MX and A records on the DNS server for each domain IronMail proxies must be captured. IronMail will store this information in its own database and use it to compare the current MX and A records when it checks the DNS server at the user-defined interval. The DNS Hijack Protection page offers the following options:

Click **Get Snapshot** to query the DNS server(s) and *write the MX and A record information to IronMail's database*. Within a few moments the MX information for each domain IronMail hosts is displayed. IronMail will now monitor each domain listed in this table for possible DNS Hijacking. If for any reason it is decided that IronMail should stop monitoring the MX information for a domain, select its **Delete** check box and click **Submit**.

If the MX and A record of a mail server ever change for a valid reason, remember to update IronMail's database by taking a new snapshot of the DNS records.

Click **Submit** when done.

If at some future time IronMail is configured to host additional mail servers (added in *Mail-Firewall > Mail Routing > Domain-based*), return to this page in order to capture a fresh snapshot of the new mail servers' MX and A records. Note that when doing so, IronMail will re-introduce into this table MX and A record information for domains that may have been previously deleted. If a domain was previously removed from DNS Hijack Protection, remember to "delete" it once again after the new snapshot is taken.

IronMail Alerts

Alert Levels

The possible alerts IronMail can send are as follows:.

- **Information:** (This alert is for information only. No problem exists. It reports, for example, that an SNMP heartbeat has been sent.)
- **Notification:** (This alert is slightly more important than "information." It reports information about an IronMail process or service. For example, it reports that an anti-virus update has been received.)
- **Warning:** (A warning should "get your attention." It implies that administrative action is warranted. For example, IronMail generates a warning when a Denial of Service attack has been detected.)
- **Error:** (An error is serious. IronMail generates error messages when a single process is not performing as intended. For example, it generates an error alert if it detects that IronMail's Content Filtering Queue stops processing messages.)
- **Critical:** (A critical alert is even more serious. IronMail generates this alert when an error affects the entire appliance. It reports, for example, when IronMail cannot reach a *DNS server*.)
- **Shutdown**: (This alert is reserved for future functionality.)
- **Restart:** (This alert is reserved for future functionality.)

Alert Manager

IronMail continuously monitors its core subsystems, as well as its ability to communicate with internal mail servers. If any part of IronMail's functionality fails to perform as designed, IronMail will generate an "alert." The alerts, by themselves, don't do anything. Rather, the Alert Manager—which processes all IronMail-generated alerts—must be configured to send them to an administrator.

IronMail's alert management is configured on the basis of two groups:

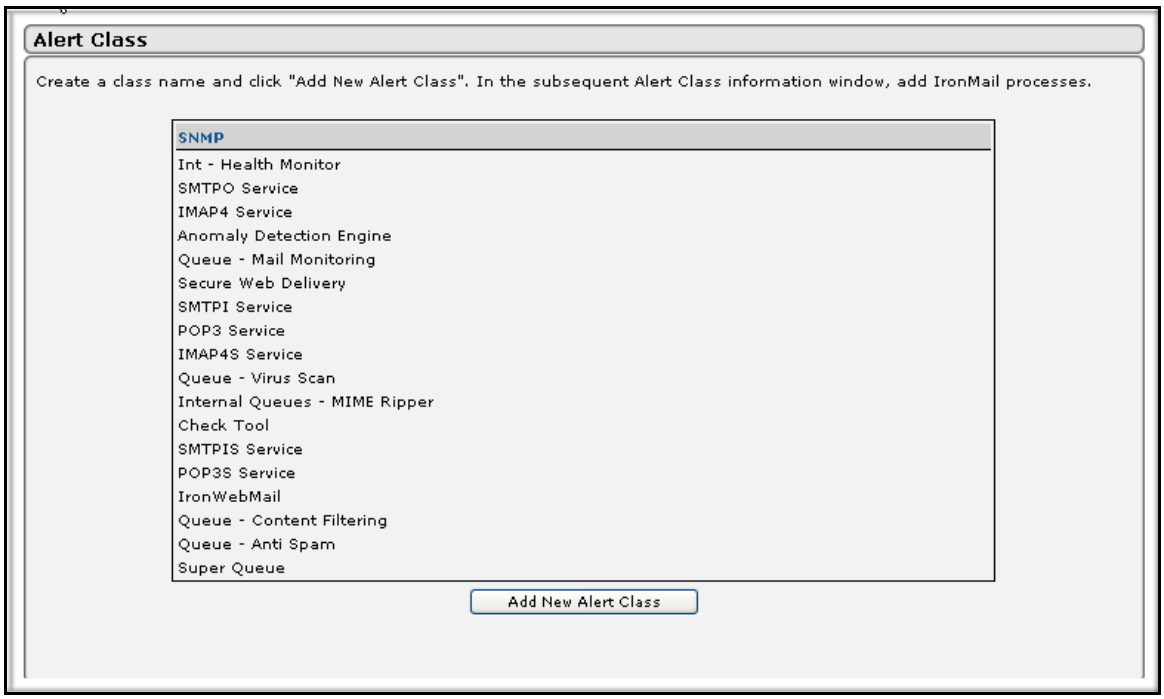
- **IronMail subsystems:** The IronMail application is comprised of eighteen core subsystems. Each one is designed to generate alerts when anomalous conditions are experienced. Administrators will create logical groupings of these subsystems.
- **Alert Levels:** IronMail is designed to look for specific types of problems—such as a subsystem stopping unexpectedly, or restarting after it was stopped. There are a finite number of anomalies that IronMail can report on (see the table of alerts). Each anomaly may be assigned one of seven "alert levels" according to the degree of criticality of the problem.

IronMail administrators will create an alert mechanism (email, pager, SNMP trap) for any or all of the "alert levels," for each grouping of subsystem they have created.

The Alert Manager hyperlink in the left navigation frame of the Web Administration interface expands to offer Alert Class, Alert Mechanism, and Alert Viewer sub-menus.

Alert Class

The Alert Class screen allows the Administrator to define groups of related services. Groups may be added, edited and deleted, and services may be assigned and reassigned to groups through this functionality. The Alert Class window is accessed through the Alert Manager menu.



By default, IronMail starts with one logical grouping, or "class," of subsystems: SNMP. Administrators may create any logical grouping of services that serves their needs. Individual subsystems may be moved from one grouping or "class" to another or deleted altogether. The purpose of creating classes of subsystems is to be "granular" in terms of which alert notifications are received, as will be explained below. When the classes have been added, Alert Levels may be configured for them using the Alert Mechanism function.

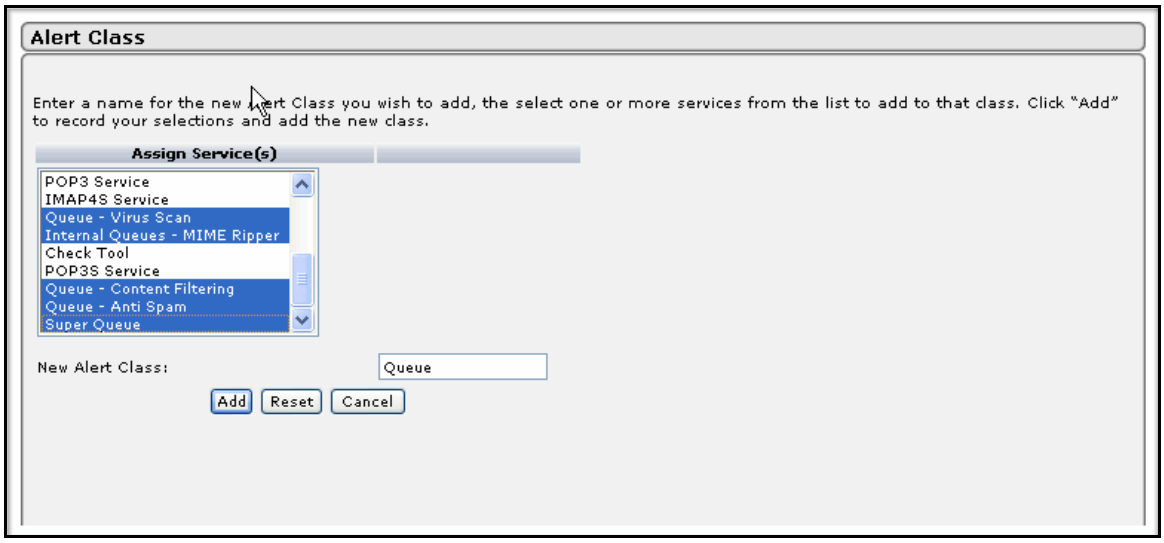
If a subsystem is deleted from a group and not added to another, IronMail will automatically create a class named "Common" and place the unused subsystem there. Alerts that might be generated by a subsystem in the Common class are not delivered to an administrator unless an alert mechanism for the Common class is created.

The following examples show possible groups or classes that may be desirable, and list the possible subsystems that might be included.

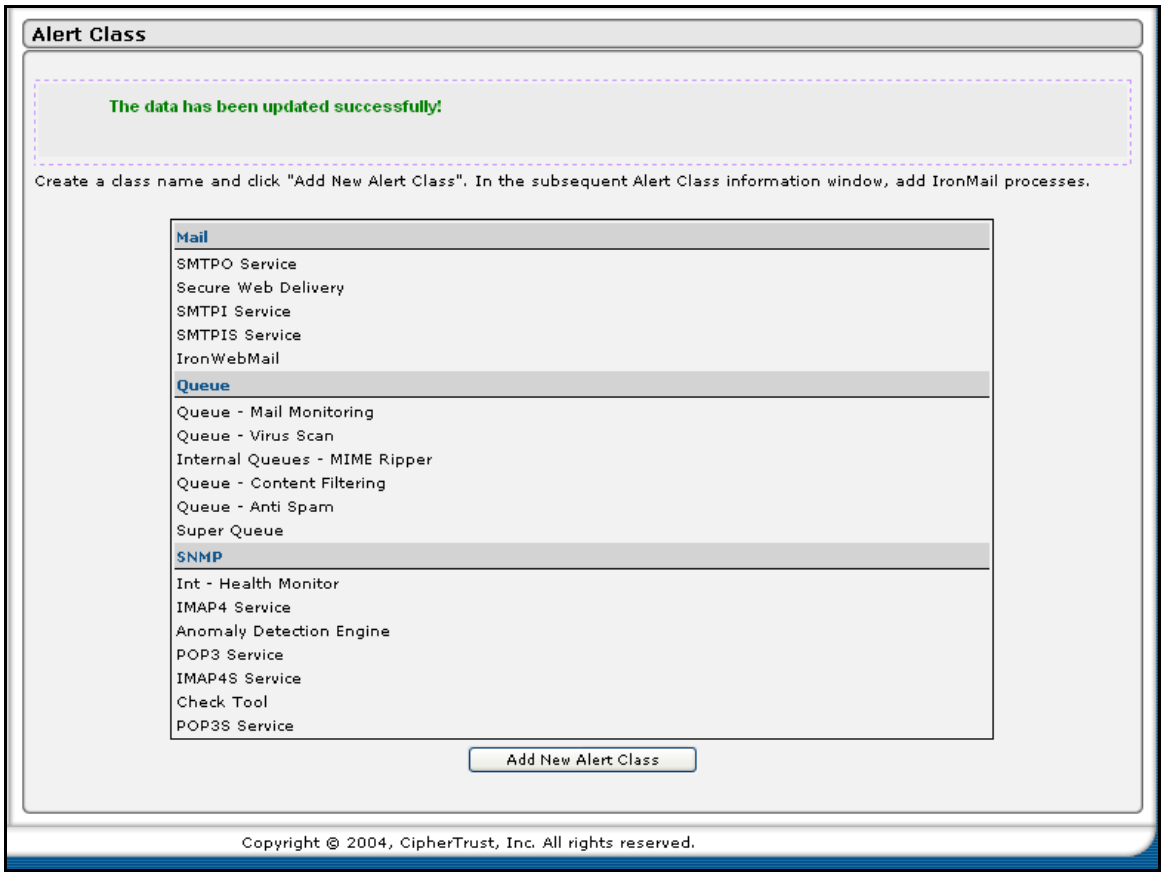
- **AV:** The Virus Scan queue.
- **Mail:** The SMTPO Service, SMTPI Service, SMTPIS Service, and IronWebMail Service all address "message delivery."
- **Monitor:** The Int – Health, Anomaly Detection Engine, and Check Tool all generally address the protection of IronMail, and ensuring that it runs as designed.
- **Proxies:** The *IMAP4* Service, *POP3* Service, IMAP4S Service, and POP3S Service all address message retrieval.
- **Queue:** The Mail Monitoring Queue, Content Filtering Queue, Virus Scan Queue, Anti Spam Queue, Internal Queues (Rip and Join), and Secure Web Delivery all address message processing and email *policy* enforcement.

Adding an Alert Class

Adding a new class begins when the Administrator clicks the Add New Alert Class button and the bottom of the Alert Class Screen. The following screen opens.


Alert Class
Enter a name for the new Alert Class you wish to add, the select one or more services from the list to add to that class. Click "Add" to record your selections and add the new class.
Assign Service(s)
POP3 Service
IMAP4S Service
Queue - Virus Scan
Internal Queues - MIME Ripper
Check Tool
POP3S Service
Queue - Content Filtering
Queue - Anti Spam
Super Queue
New Alert Class:
Queue
Add
Reset
Cancel

To add the new class, enter the name for the class in the New Alert Class data field, then select from the scrolling list one or more services to be included in the class. Click **Add** when the selection is finished. The screen will refresh.

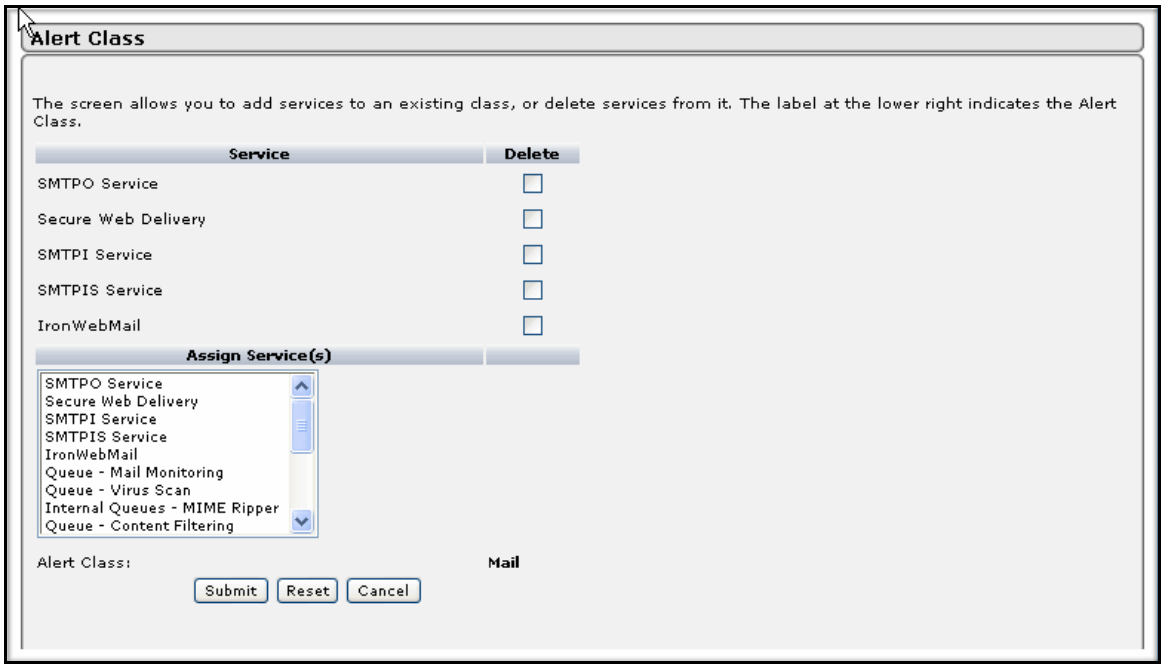


The screen displays the name of each Alert Class and, underneath the name, the list of subsystems assigned to that class.

The Administrator may now configure the alerts for the class.

Editing an Alert Class

The name of each Alert Class on the screen is a hyperlink that allows the Administrator to edit that class. When one clicks the name hyperlink, the following screen opens.

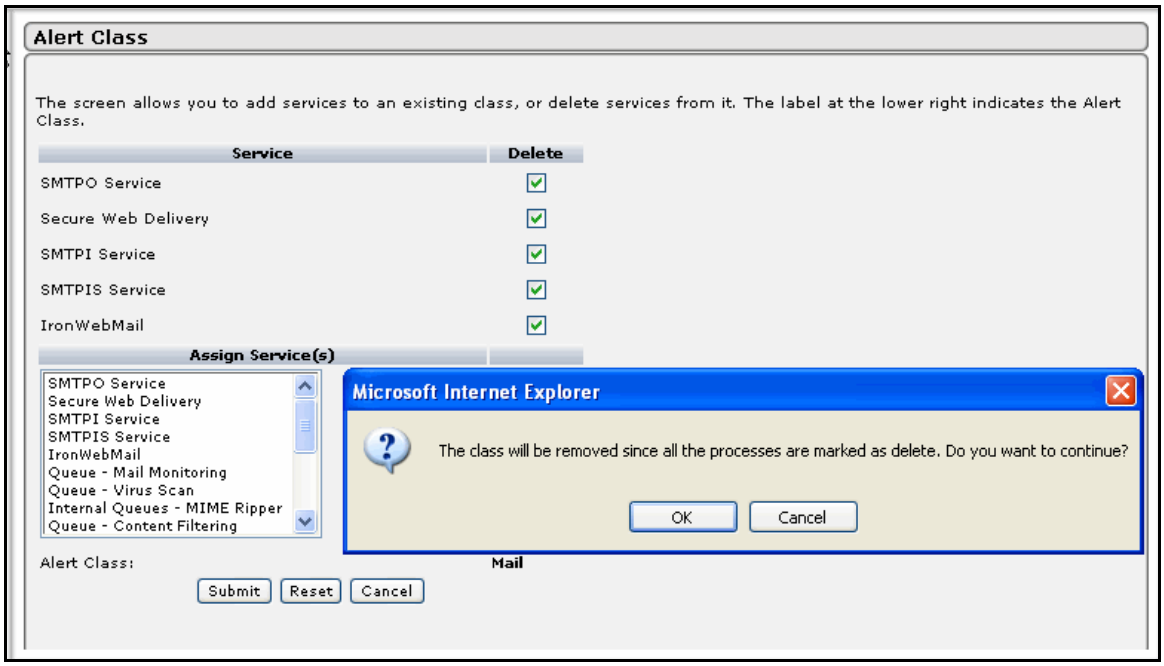


The screen contains the following information:

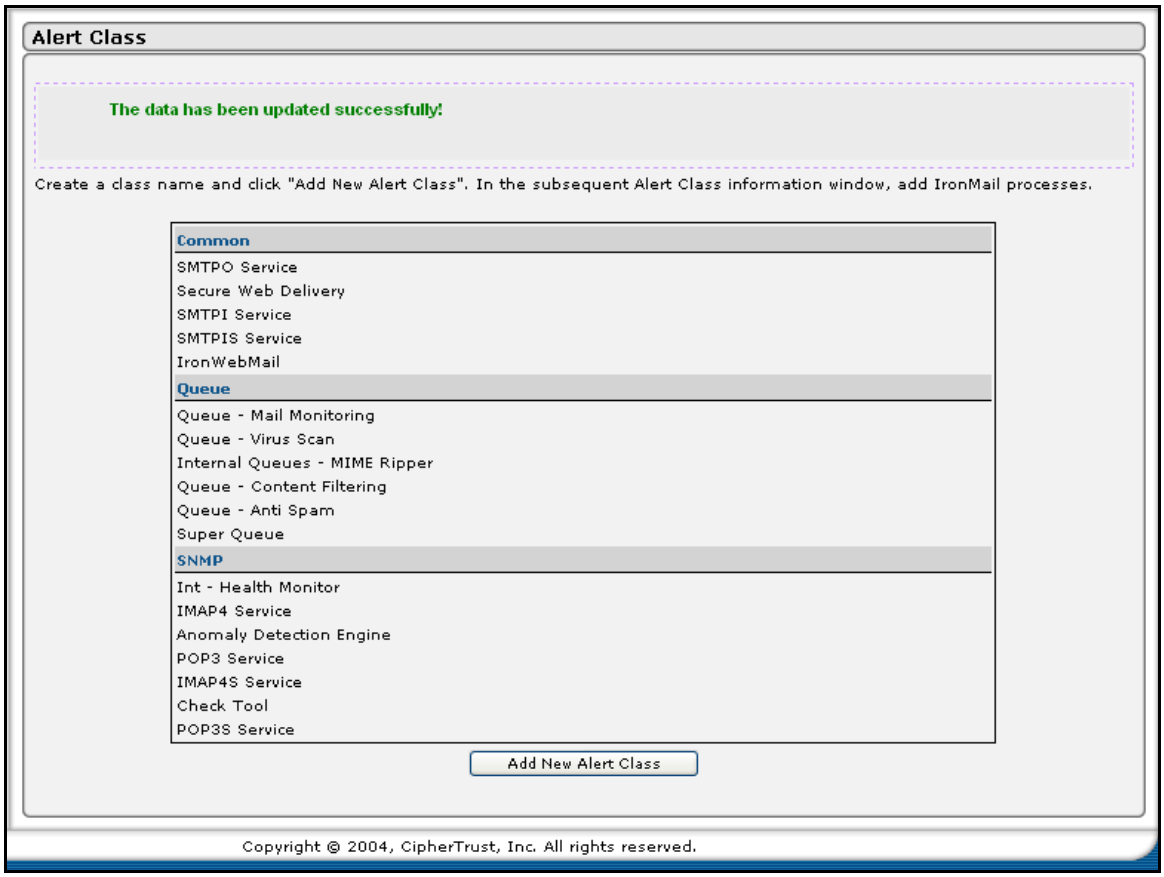
Field	Description
Service	The column shows the current list of subsystems assigned to the class.
Delete	Checking the Delete checkbox for any subsystem will delete that subsystem from the class.
Assign Services	This column shows all the services. Select one or more of them (click, Ctrl-click or Shift-click) to be added to the class.
Alert Class:	The name of the Alert Class shows at the lower middle part of the screen.

Make the required changes to the screen, and click **Submit.** The Alert Class screen will refresh.

To delete an entire class from the list, check the Delete boxes for all services in that class and click **Submit**.



A confirmation alert will appear; click OK. The screen will refresh.



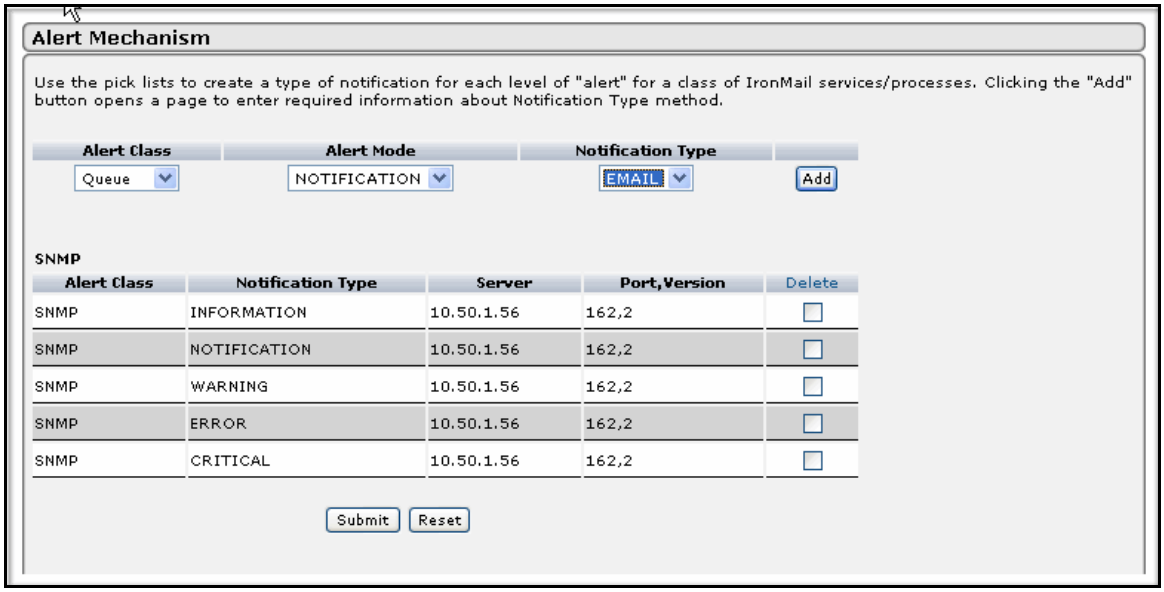
If the Administrator wants to see certain types of alerts—for example, "Information" alerts—for one subsystem, and not for others, that subsystem should be in a class all by itself. Otherwise,

when an alert mechanism is created for the purpose of sending “Information” alerts for a class, IronMail will send “Information” alerts generated by all subsystems within the class.

After alert classes have been created, navigate to *Administration> Alert Manager > Alert Mechanism* to specify how the alerts are to be delivered.

Alert Mechanism

The Alert Mechanism page is where Alert Manager is configured to send alerts to the administrator by email, pager, or SNMP traps. An alert mechanism must be configured for each level of alert, and for each group or “class” of IronMail subsystems for which the administrator wants notification. For example, if administrators want to be notified whenever the SMTPO Service stops performing (reported as an “Error” alert by IronMail), an “Error” email, pager, or SNMP alert mechanism must be configured for the class that contains the SMTPO Service. Conversely, if alert mechanisms for “Information” alerts are not created for a particular class, no “Information” alerts for any subsystem within that class will be sent to the administrator.



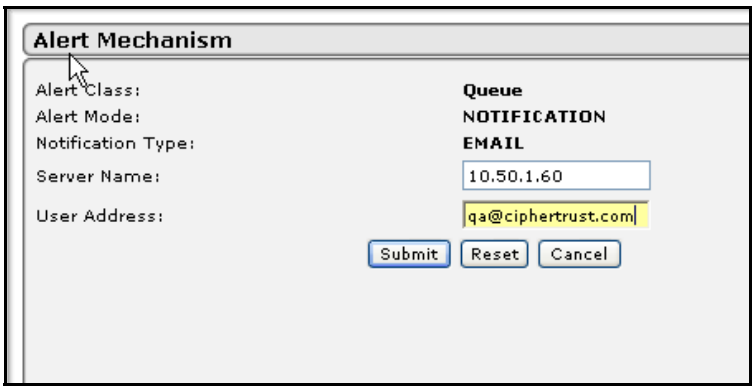
The Alert Mechanism page contains three pick lists allowing configuration of alerts notifications, and displays a table of all configured alerts.

Field	Description
Alert Class	The **Alert Class** pick list contains the names of all classes of subsystems that have been created. (IronMail creates a default “Common” class to contain unused subsystems.) Select a class from the list, and then select related values in the **Alert Type** and **Notification Type** pick lists.
Alert Mode	The pick list contains the seven Alert Levels that IronMail can generate. Select an alert level from the list. Options are: • **Information:** (This alert is for information only. No problem exists. It reports, for example, that an SNMP heartbeat has been sent.) • **Notification:** (This alert is slightly more important than “information.” It reports information about an IronMail process or service. For example, it reports that an anti-virus update has been received.) • **Warning:** (A warning should “get your attention.” It implies that administrative action is warranted. For example, IronMail generates a

	warning when a Denial of Service attack has been detected.) • **Error:** (An error is serious. IronMail generates error messages when a single process is not performing as intended. For example, it generates an error alert if it detects that IronMail's Content Filtering Queue stops processing messages.) • **Critical:** (A critical alert is even more serious. IronMail generates this alert when an error affects the entire appliance. It reports, for example, when IronMail cannot reach a *DNS server*.) • **Shutdown**: (This alert is reserved for future functionality.) • **Restart:** (This alert is reserved for future functionality.) For each class, select a level or type of alert as well as a Notification Type.
Notification Type	The **Notification Type** pick list offers three choices for alert delivery: • Email - one or more email addresses will be required. • Pager - requires the *host name* of the server that processes pager messaging, plus one or more pager addresses. (Multiple pager addresses must be separated from each other with commas. Do not enter spaces between commas and subsequent addresses.) • SNMP - requires the host name of the SNMP server, the port number through which communication with it occurs, and the version number of the SNMP application.
Add	Click this button to set up a new Alert Mechanism.
Table of Existing Mechanisms	***The lower portion of the screen contains a listing of the Alert Mechanisms that have been configured.***
Alert Class	This column shows all classes for which alerts have been configured.
Notification Type	The column lists the types of alerts that have been established for each class.
Server	The name (IP address) of the server to which the notice is sent is shown in this column
Port, Version	The column displays the port number and SNMP version for each Alert Mechanism.
Delete	Clicking the Delete box and clicking **Submit** will cause the mechanism to be deleted from IronMail.

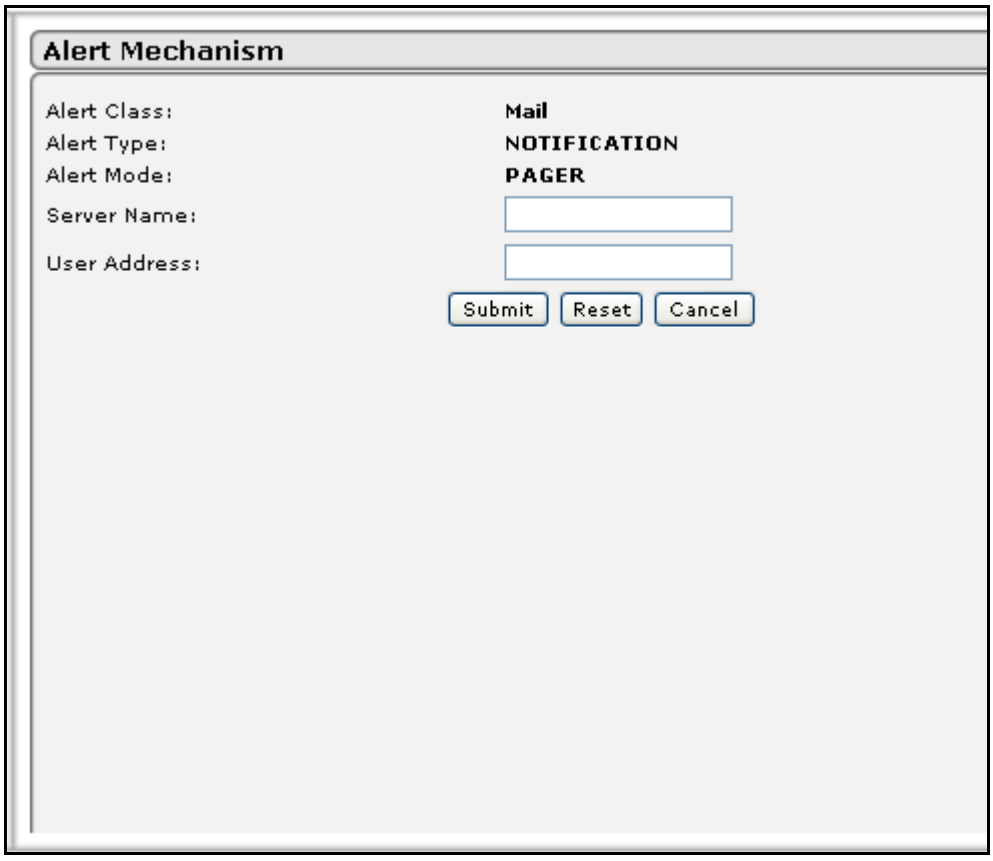
Adding a New Notification

After selecting an alert mechanism configuration, click **Add**. A window opens where information about the mechanism must be provided. The window below allows configuring an email mechanism.



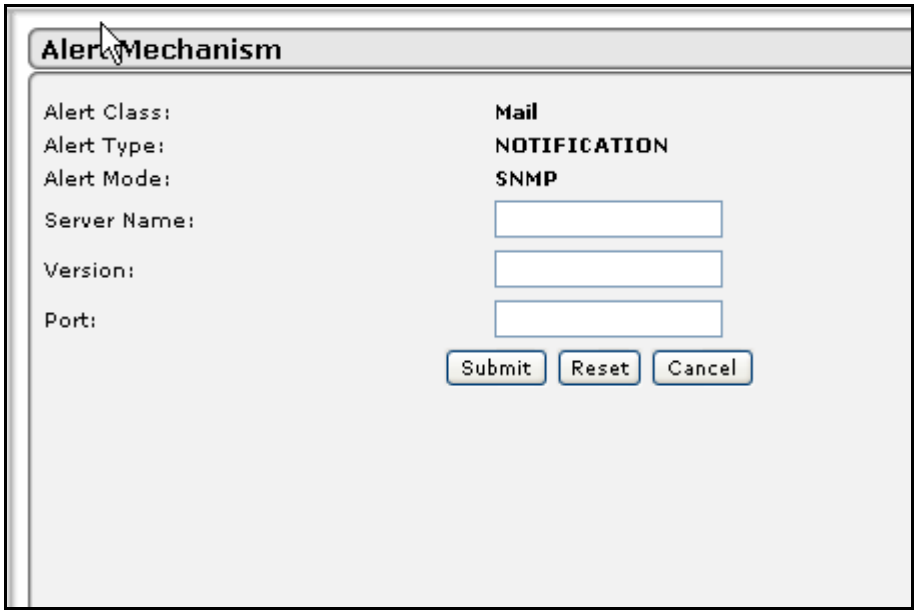
Field	Description
Alert Class	Pre-populated with the name of the mechanism being added.
Alert Mode	Pre-populated with the selected mode.
Notification Type	Pre-populated with the selected means for delivering the alerts.
Server Name	Enter the server name/IP address to which the alert is to be sent.
User Address	Enter the email address for the recipient of the alerts. Multiple email addresses must be separated from each other with commas. Do not enter spaces between commas and subsequent email addresses.

If a Notification Type of Pager is selected, this screen opens.



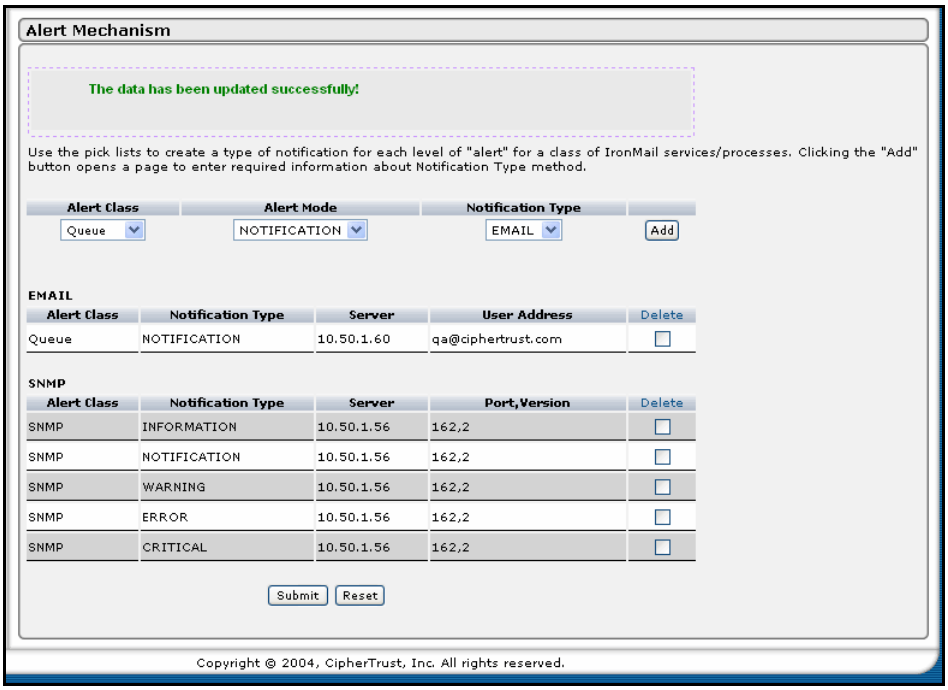
Field	Description
Alert Class	Pre-populated with the name of the mechanism being added.
Alert Mode	Pre-populated with the selected mode.
Notification Type	Pre-populated with the selected means for delivering the alerts.
Server Name	Enter the server name for the pager.
User Address	Enter the pager number for the recipient of the alerts. Multiple pager numbers must be separated from each other with commas. Do not enter spaces between commas and subsequent pager numbers.

If SNMP is the method for delivering the alerts, the configuration is completed on this screen.



Field	Description
Alert Class	Pre-populated with the name of the mechanism being added.
Alert Mode	Pre-populated with the selected mode.
Notification Type	Pre-populated with the selected means for delivering the alerts.
Server Name	Enter the server name/IP address to which the alert is to be sent.
Version	Enter the version number for the version of SNMP that is being used.
Port	Enter the port number for the SMNP server.

Click **Submit** to save the configuration. The main Alert Mechanism screen will be updated.

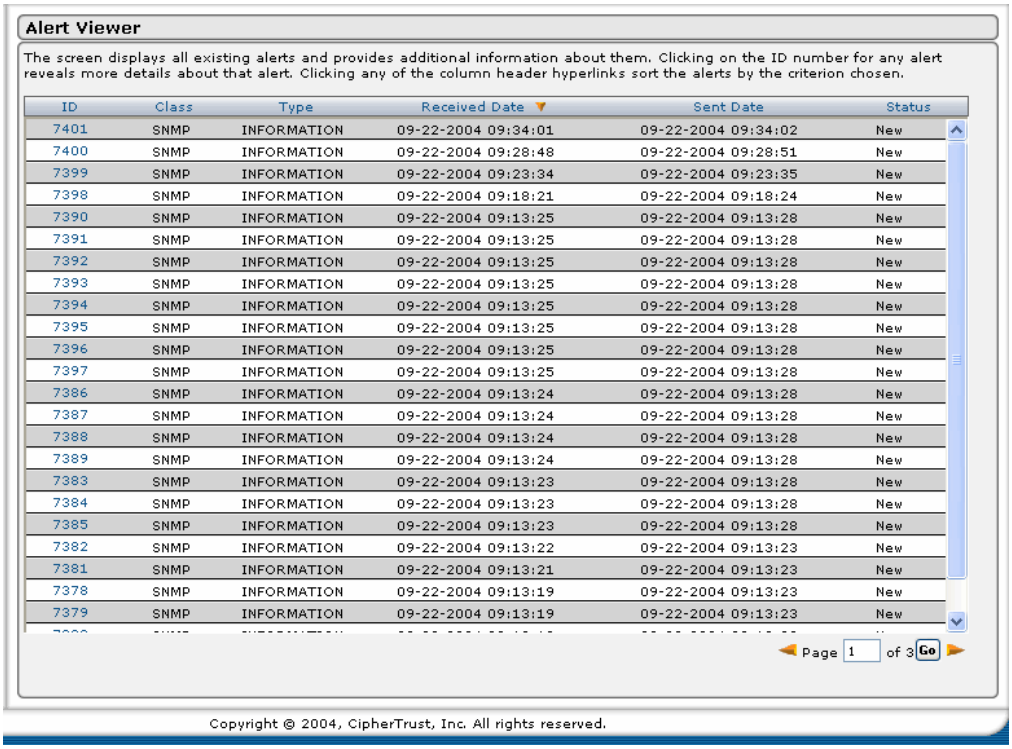


Editing an Alert Mechanism

To edit an Alert Mechanism, the Administrator must delete it from the main Alert Mechanism screen and re-add it with the new configuration.

Alert Viewer

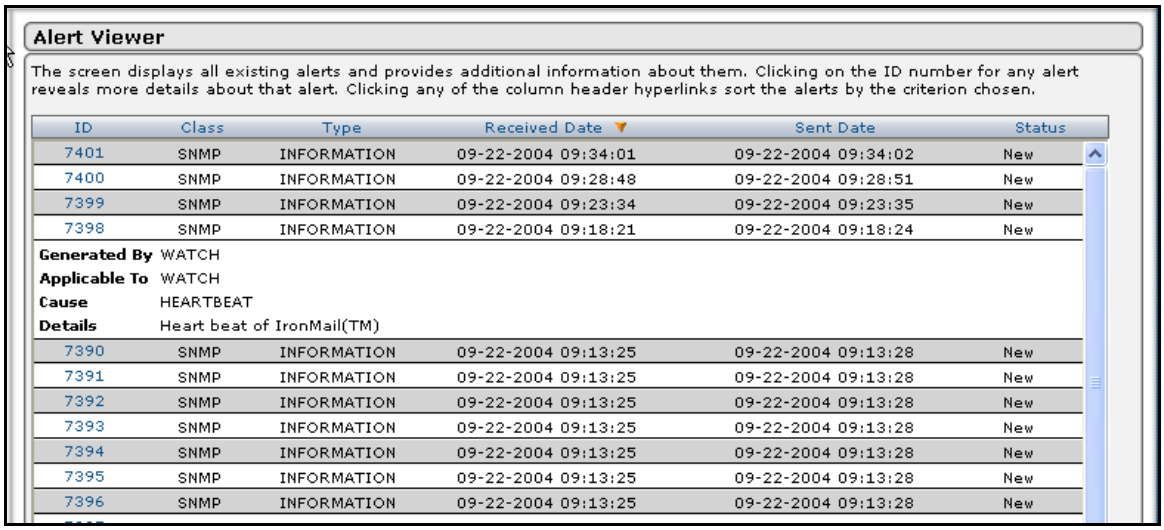
The Alert Viewer page allows administrators to view, on-screen, all the alerts that IronMail generated in the previous three hours. (IronMail automatically deletes old alert information unattended in the background.)



The Alert Viewer displays the following information:

Field	Description
ID	This column displays the internally-generated ID number of each alert. The ID number is also a hyperlink that opens a secondary browser window displaying details of the alert.
Class	This column displays the name of the class that contains the subsystem that generated the alert. The Class column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by class in ascending and descending order.
Type	This column identifies the level of the alert. The Type column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by alert level in ascending and descending order.
Received Date	This column identifies the timestamp when the alert was generated. The Received Date column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Received Date in ascending and descending order.
Sent Date	This column identifies the timestamp when the alert was delivered. The Sent Date column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Sent Date in ascending and descending order.
Status	This column identifies the "status" of the alert, and will display one of two values: • **Delivered:** IronMail successfully delivered the alert. • **Not Delivered:** IronMail was not successful in delivering the alert. The Status column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Status in ascending and descending order.

When the alert ID hyperlink in the Alert Viewer table is clicked, a secondary browser window opens, displaying information about the alert.


Alert Viewer
The screen displays all existing alerts and provides additional information about them. Clicking on the ID number for any alert reveals more details about that alert. Clicking any of the column header hyperlinks sort the alerts by the criterion chosen.
ID Class Type Received Date Sent Date Status
7401 SNMP INFORMATION 09-22-2004 09:34:01 09-22-2004 09:34:02 New
7400 SNMP INFORMATION 09-22-2004 09:28:48 09-22-2004 09:28:51 New
7399 SNMP INFORMATION 09-22-2004 09:23:34 09-22-2004 09:23:35 New
7398 SNMP INFORMATION 09-22-2004 09:18:21 09-22-2004 09:18:24 New
Generated By WATCH
Applicable To WATCH
Cause HEARTBEAT
Details Heart beat of IronMail(TM)
7390 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7391 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7392 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7393 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7394 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7395 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New
7396 SNMP INFORMATION 09-22-2004 09:13:25 09-22-2004 09:13:28 New

Field	Description
Generated by	IronMail displays the name of the subsystem that generated the alert.
Applicable to	For all subsystems except Health Monitor, the reported value will be "Self." That is, the subsystem generating the alert reports a condition about its own operation. Health Monitor, on the other hand, is capable of generating alerts related to other subsystems. Therefore, when Heath Monitor generates an alert, it will report the name of the subsystem that is experiencing the specified condition.
Cause	The "name" of the alert is reported. See the table of alerts for a complete description of the individual alerts IronMail is capable of generating.
Details	Specific information about the alert condition is reported.

Table of IronMail-generated Alerts

IronMail automatically generates a variety of Alerts for the following subsystems:

Subsystem	Explanation
Anomaly Detection	The Anomaly Detection Engine looks historically at your email activity and detects "patterns" or "events" that you define.
Anti-Virus Queue	The Anti-Virus Queue scans messages for viruses.
Content Filtering Queue	The Content Filtering Queue looks for "keywords" within emails and attachments and takes user-defined action accordingly.
Mail Monitoring Queue	The Mail Monitoring Queue applies a variety or rules to messages, such as checking to whom it is addressed or from whom it was sent.
Spam Queue	The Spam Queue uses a variety of technologies to discover whether messages are spam or not, such as performing reverse DNS, RBL, Razor and Statistical Lookup Service (SLS) lookups.
Health Monitor	Health Monitor examines IronMail's performance, running a series of tests to ensure that all its services are performing as intended.
Internal Queues	Before messages even enter the Anti-Virus, Anti-Spam, Content Filtering or Mail Monitoring Queues, a "Rip Queue" rips messages into their separate *MIME* parts. Similarly, when all the queues have finished processing messages, a "Join Queue" reassembles each message.
SMTPI Service	The SMTPI Service processes all non-secure mail being delivered to the IronMail appliance.
SMTPIS Service	The SMTPIS Service processes all secure mail being delivered to the IronMail appliance.
SMTPO Service	The SMTPO Service processes all mail delivered outside the IronMail appliance.
POP3 Service	The POP3 Service processes all non-secure POP3 mail retrieval requests.
POP3S Service	The POP3S Service processes all secure POP3 mail retrieval requests.
IMAP4 Service	The IMAP4 Service processes all non-secure IMAP4 mail retrieval

	requests.
IMAP4S Service	The IMAP4S Service processes all secure IMAP4 mail retrieval requests.
IronWebMail	IronWebMail provides protection for browser-based email (protection against HTTP *network* attacks).
SWM Queue	The SWM queue holds all emails for Secure Delivery.
Update Processes	Update processes are used to ensure that the most current versions of features and functionality are available in the proper versions of IronMail.

The following table lists every alert IronMail is capable of generating:

IronMail Processes	**Cause**	**Alert Text**	**Alert type**
Health Monitor	Heartbeat	"Heartbeat Trap"	**Information** When IronMail generates a heartbeat for your SNMP console, it can generate an information alert.
Health Monitor	SMTPO Up	"SMTP Out UP Trap"	**Notification** When IronMail restarts the SMTPO (outbound delivery) service after a failure, it can generate a notification alert.
Health Monitor	SMTPO Down	"SMTP Out DOWN Trap"	**Error** If IronMail has to shut down the SMTPO (outbound delivery) service due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	SMTPO Error	"SMTP Out ERROR Trap"	**Warning/Error** If the SMTPO (outbound delivery) service experiences other errors, IronMail can generate either warning or error alerts. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	SMTPPROXY Up	"SMTPPROXY UP Trap"	**Notification** When IronMail restarts the SMTPI (incoming delivery) service after a failure, it can send a notification alert.
Health Monitor	SMTPPROXY Down	"SMTPPROXY DOWN Trap"	Error If IronMail has to shut down the SMTPI (incoming delivery) service due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	SMTPPROXY Error	"SMTPPROXY ERROR Trap"	**Warning/Error** If the SMTPI (incoming delivery) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	SMTPPROXY Restart	"SMTPPROXY RESTART Trap"	Notification When IronMail restarts the SMTPPROXY service, it can generate a notification alert.
Health Monitor	SMTPSPROXY Up	"SMTPSPROXY UP Trap"	**Notification** When IronMail restarts the SMTPIS (secure incoming delivery) service after a failure, it can generate a notification alert.
Health Monitor	SMTPSPROXY Down	"SMTPSPROXY DOWN Trap"	**Error** If IronMail has to shut down the SMTPIS (secure incoming delivery) service due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	SMTPSPROXY-Error	"SMTPSPROXY ERROR Trap"	**Warning/Error** If the SMTPIS (secure incoming delivery) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	SMTPSPROXY Restart	"SMTPSPROXY RESTART Trap"	**Notification** When IronMail restarts the SMPTI service, it can generate a notification.
Health Monitor	POP3PROXY-Up	"POP3PROXY UP Trap"	**Notification** When IronMail restarts the *POP3* (message retrieval) service after a failure, it can generate a notification alert.
Health Monitor	POP3PROXY-Down	"POP3PROXY DOWN Trap"	**Error** If IronMail has to shut down the POP3 (message retrieval) service due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	POP3PROXY-Error	"POP3PROXY ERROR Trap"	**Warning/Error** If the POP3 (message retrieval) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	POP3PROXY Restart	"POP3PROXY RESTART Trap"	Notification When IronMail restarts the POP3PROXY service, it can generate a notification.
Health Monitor	POP3SPROXY-Up	"POP3SPROXY UP Trap"	**Notification** When IronMail restarts the POP3S (secure message retrieval) service after a failure, it can generate a notification alert.
Health Monitor	POP3SPROXY-Down	"POP3SPROXY DOWN Trap"	**Error** If IronMail has to shut down the POP3S (secure message retrieval) service due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	POP3SPROXY-Error	"POP3SPROXY ERROR Trap"	**Warning/Error** If the POP3S (secure message retrieval) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	POP3SPROXY Restart	"POP3SPROXY RESTART Trap"	Notification When IronMail restarts the POP3PROXY service, it can generate a notification.
Health Monitor	IMAP4PROXY-Up	"IMAP4PROXY UP Trap"	**Notification** When IronMail restarts the *IMAP4* (message retrieval) service after a failure, it can generate a notification alert.
Health Monitor	IMAP4PROXY-Down	"IMAP4PROXY DOWN Trap"	**Error** If IronMail has to shut down the IMAP4 (message retrieval) service due to memory load or other factors, it can generate an error alert.

Health Monitor	IMAP4PROXY-Error	"IMAP4PROXY ERROR Trap"	**Warning/Error** If the IMAP4 (message retrieval) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	IMAP4PROXY Restart	"IMAP4PROXY RESTART Trap"	**Notification** When IronMail restarts the IMAP4PROXY service, it can generate a notification.
Health Monitor	IMAP4SPROXY-Up	"IMAP4SPROXY UP Trap"	**Notification** When IronMail restarts the IMAP4S (secure message retrieval) service after a failure, it can generate a notification alert.
Health Monitor	IMAP4SPROXY-Down	"IMAP4SPROXY DOWN Trap"	**Error** If IronMail has to shut down the IMAP4S (secure message retrieval) service due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	IMAP4SPROXY-Error	"IMAP4SPROXY ERROR Trap"	**Warning/Error** If the IMAP4S (secure message retrieval) service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	IMAP4SPROXY Restart	"IMAP4SPROXY RESTART Trap"	**Notification** When IronMail restarts the IMAP4SPROXY service, it can generate a notification.
Health Monitor	HTTPD-Up	"HTTPD UP Trap"	**Notification** When IronMail restarts its web server (running the web-based graphical user interface) after a failure, it can generate a notification alert.
Health Monitor	HTTPD-Down	"HTTPD DOWN Trap"	**Error** If IronMail's web server (running the web-based graphical user interface) shuts down due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	HTTPD-Error	"HTTPD ERROR Trap"	**Warning/Error** If IronMail's web server (running the web-based graphical user interface) experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	HTTPD Restart	"HTTPD RESTART Trap"	**Notification** When IronMail restarts the HTTPD service, it can generate a notification.
Health Monitor	Tomcat-Up	"TOMCAT UP Trap"	**Notification** When IronMail restarts the JSP interpreter (powering the browser interface) after a failure, it can generate a notification alert.
Health Monitor	Tomcat-Down	"TOMCAT DOWN Trap"	**Error** If IronMail's JSP interpreter (powering the browser interface) shuts due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	Tomcat-Error	"TOMCAT ERROR Trap"	**Warning/Error** If IronMail's JSP interpreter (powering the browser interface) experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Tomcat Restart	"TOMCAT RESTART Trap"	
Health Monitor	Content Filtering Queue-Up	"CFQ UP Trap"	**Notification** When IronMail restarts the Content Filtering Queue after a failure, it can generate a notification alert.
Health Monitor	Content Filtering Queue-Down	"CFQ DOWN Trap"	**Error** If IronMail's Content Filtering Queue shuts due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	Content Filtering Queue-Error	"CFQ ERROR Trap"	**Warning/Error** If IronMail's Content Filtering Queue experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Content Filtering Queue Restart	"CFQ RESTART Trap"	**Notification** When IronMail restarts the Content Filtering Queue, it can generate a notification.
Health Monitor	Anti-Virus Queue-Up	"AVQ UP Trap"	**Notification** When IronMail restarts the Anti-Virus Queue after a failure, it can generate a notification alert.
Health Monitor	Anti-Virus Queue-Down	"AVQ DOWN Trap"	**Error** If IronMail's Anti-Virus Queue shuts due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	Anti-Virus Queue-Error	"AVQ ERROR Trap"	**Warning/Error** If IronMail's Anti-Virus Queue experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Anti-Virus Queue Restart	"AVQ RESTART Trap"	**Notification** When IronMail restarts the Anti-Virus Queue, it can generate a notification.
Health Monitor	Rip Queue-Up	"RIPQ UP Trap"	**Notification** When IronMail restarts the Rip Queue (responsible for separating a message into its individual *MIME* parts) after a failure, it can generate a notification alert.
Health Monitor	Rip Queue-Down	"RIPQ DOWN Trap"	**Error** If IronMail's Rip Queue (responsible for separating a message into its individual MIME parts) shuts down due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	Rip Queue-Error	"RIPQ ERROR Trap"	**Warning/Error** If IronMail's Rip Queue (responsible for separating a message into its individual MIME parts) experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Rip Queue Restart	"RIPQ RESTART Trap"	**Notification** When IronMail restarts the Rip Queue, it can generate a notification.
Health Monitor	Mail Monitoring Queue-Up	"MMQ UP Trap"	**Notification** When IronMail restarts the Mail Monitoring Queue after a failure, it can generate a notification alert.
Health Monitor	Mail Monitoring Queue-Down	"MMQ DOWN Trap"	**Error** If IronMail's Mail Monitoring Queue shuts down due to excessive memory load or other factors, it can generate an error alert.
Health Monitor	Mail Monitoring Queue-Error	"MMQ ERROR Trap"	**Warning/Error** If IronMail's Mail Monitoring Queue experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Mail Monitoring Queue Restart	"MMQ RESTART Trap"	**Notification** When IronMail restarts the Mail Monitoring Queue, it can generate a notification.
Health Monitor	Join Queue-Up	"JOINQ UP Trap"	**Notification** When IronMail restarts the Join Queue (responsible for putting the MIME parts back together again) after a failure, it can generate a notification alert.
Health Monitor	Join Queue-Down	"JOINQ DOWN Trap"	**Error** If IronMail's Join Queue (responsible for putting the MIME parts back together again) shuts down due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	Join Queue-Error	"JOINQ ERROR Trap"	**Warning/Error** If IronMail's Join Queue (responsible for putting the MIME parts back together again) experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Join Queue Restart	"JOINQ RESTART Trap"	**Notification** When IronMail restarts the Join Queue, it can generate a notification.
Health Monitor	Disk-Up	"SYS-DISK UP Trap"	**Notification** Each time IronMail is restarted, it can generate a notification alert that the hard disk utilization is less than the user-defined threshold. (It will not generate subsequent "up" alerts unless the appliance is restarted.)
Health Monitor	Disk Down	"SYS-DISK DOWN Trap"	**Error** Each time the hard disk shuts down, IronMail can generate an error alert.
Health Monitor	Disk-Error	"SYS-DISK ERROR Trap"	**Warning/Error** If IronMail's user-defined disk utilization threshold has been reached, either a warning or error message can be generated. (IronMail intelligently monitors the disk space values and escalates the alerts accordingly.)
Health Monitor	Cryptocard-Up (not all IronMail models)	"SYS-DISK CRYPTO UP Trap"	**Notification** Each time IronMail is restarted, it can generate a notification that the cryptographic accelerator card is functioning normally. (It will not generate subsequent "up" alerts unless the appliance is restarted.)
Health Monitor	Cryptocard-Down (not all IronMail models)	"SYS-DISK CRYPTO DOWN Trap"	**Error** If IronMail detects abnormal performance in the cryptographic accelerator card, it can generate an error alert.

Health Monitor	Cryptocard-Error (not all IronMail models)	"SYS-DISK CRYPTO ERROR Trap"	**Warning/Error** If IronMail detects serious errors in the cryptographic accelerator card, either a warning or error message can be generated. (IronMail intelligently monitors the performance values and escalates the alerts accordingly.)
Health Monitor	*Network* Status Up	"SYS-NETSTAT UP Trap"	**Notification** When IronMail restarts the Network Status service, it can generate a notification.
Health Monitor	Internal Server-Up	"INTERNAL-SERVER UP Trap"	**Notification** Each time IronMail is restarted, it can send a notification that the internal mail server is responding normally. (It will not generate subsequent “up” alerts unless the internal mail server is restarted.)
Health Monitor	Internal Server-Down	"INTERNAL SERVER DOWN Trap"	**Error** Each time the internal mail server shuts down, IronMail can send an error notification.
Health Monitor	Internal Server-Error	"INTERNAL SERVER ERROR Trap"	**Warning/Error** If the internal mail server fails to respond, IronMail can generate either a warning or error alert.
Health Monitor	DNS Hijack-Up	"SYS-DNSHIJACK UP Trap"	**Notification** When IronMail restarts DNS Hijack protection, it can send a notification that the protection is responding normally.
Health Monitor	DNS Hijack-Down	"SYS-DNSHIJACK DOWN Trap"	**Error** If IronMail's DNS Hijack protection shuts down, IronMail can send an error message.
Health Monitor	DNS Hijack Error	"SYS-DNSHIJACK ERROR Trap"	**Warning/Error** If the DNS Hijack service experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)

Health Monitor	Command Line Interface-Up	"SSHD Console UP Trap"	**Notification** When IronMail restarts the Command Line Interface, it can send a notification that the protection is responding normally.
Health Monitor	Command Line Interface-Down	"SSHD Console DOWN Trap"	**Error** If IronMail's Command Line Interface shuts down, IronMail can send an error message.
Health Monitor	Command Line Interface-Error	"SSHD Console ERROR Trap"	**Warning/Error** If the Command Line Interface experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Support pipe-Up	"SSHD Maint UP Trap"	**Notification** When IronMail restarts the support pipe, it can send a notification that the protection is responding normally.
Health Monitor	Support pipe-Down	"SSHD Maint DOWN Trap"	**Error** If IronMail's support pipe shuts down, IronMail can send an error message.
Health Monitor	Support pipe-Error	"SSHD Maint ERROR Trap"	**Warning/Notification** If the support pipe experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Support Pipe Restart	"SSHD Maint RESTART Trap"	**Notification** When IronMail restarts the Support Pipe, it can generate a notification.
Health Monitor	Spam Queue-Up	"SPAM UP Trap"	**Notification** When IronMail restarts its Anti-Spam Queue after a failure, it can generate a notification alert.
Health Monitor	Spam Queue-Down	"SPAM DOWN Trap"	**Error** When IronMail's Anti-Spam Queue shuts down due to excessive memory load or other factors, it can generate an error alert.

Health Monitor	Spam Queue Error	"SPAM ERROR Trap"	**Warning/Error** If IronMail's Anti-Spam Queue experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)
Health Monitor	Spam Queue-Restart	"SPAM RESTART Trap"	**Notification** When IronMail restarts its Anti-Spam Queue after a failure, it can generate a notification alert.
Health Monitor	IWM Restart	"IWM RESTART Trap"	**Notification** When IronMail restarts the IWM service, it can generate a notification.
Health Monitor	Command Line Interface Restart	"SSHD Console RESTART Trap"	**Notification** When IronMail restarts the Command Line Interface, it can generate a notification.
SMTPO	TLS-Failure (SMTPO)	"SMTP Out TLS Negotiation Failure Trap"	**Warning** Whenever IronMail's SMTPO service tries and fails to establish a TLS handshake with another server, it can generate a warning alert.
SMTPO	TLS-Cert-Failure	"SMTP Out TLS Certificate Verification Failure Trap"	**Warning** If the recipient server has a Security Certificate that cannot be validated by a Trusted Root Certificate Authority, IronMail can generate a warning alert.
SMTPO	TLS-Auth-Failure	"SMTP Out Certificate Authentication Failure Trap"	**Warning** If the recipient server has a Security Certificate containing an invalid host or *domain name*, IronMail can generate a warning.
SMTPO	DNS-Failure	"SMTP Out *DNS Server* ERROR Trap"	**Notification** When the DNS server is down, IronMail can generate a critical alert.
SMTPO	DSN-Final	"SMTP Out Final DSN Intimation Trap"	**Information** When IronMail issues a final Delivery Status Notification that a message cannot be delivered, it can also generate this information alert.
SMTPO	SWM Failure	"SWM Delivery Failed"	**Notification** When Secure Web Mail is unable to deliver a message, IronMail can

			generate a notification.
SMTPI/SMTPIS	Denial of Service-Attack (SMTPI/S)	"SMTPPROXY DOS Attack Trap"	**Warning** When IronMail detects that the Denial of Service threshold has been reached via SMTPI or SMTPIS connections, it can generate a warning alert.
SMTPI/SMTPIS	TLS Failure (SMTPI/SMTPIS)	"SMTPPROXY TLS Negotiation Failure Trap"	**Information** Whenever IronMail's SMTPI or SMTPIS services fail to establish a TLS handshake with another server or client machine, it can generate a warning alert.
SMTPI/SMTPIS	Real-time Blackhole List-Failure	"STMPPROXY RBL Lookup Failure Trap"	**Notification** When IronMail receives a connection request from an *IP address* listed on an RBL list, it can generate a warning alert.
SMTPI/SMTPIS	Reverse DNS-Failure	"SMTPPROXY Reverse DNS Lookup Failure Trap"	**Notification** When a reverse DNS lookup invalidates a server or client machine, IronMail can generate a notification alert.
SMTPI/SMTPIS	Relay-Failure	"SMTPPROXY Relay Attempt Intimation Trap"	**Information** Whenever a user attempts to relay email off of IronMail but is unsuccessful, it can generate an information alert.
SMTPI/SMTPIS	Full Throttle	"SMTPPROXY Under Full Throttle Intimation Trap"	**Critical** If the IronMail Load Throttling threshold is ever reached, it can generate a critical alert.
SMTPI/SMTPIS	Auth-Failure (SMTPI/SMTPIS)	"SMTPPROXY Authentication Failure Trap"	**Information** Whenever a user is required to be authenticated, but is not, IronMail can generate an information alert.
SMTPI/SMTPIS	Deny List	"SMTPPROXY DENY List Trap"	**Warning** Whenever a connection is dropped because the sender is on IronMail's "deny" list, a warning alert can be generated.

SMTPI/SMTPIS	ESMTP Size Exceeded	"SMTPPROXY Message Exceeds Limit Trap"	**Information** Whenever a message is not accepted because the size of the message exceeds the set limit, IronMail can generate an information alert.
POP3/POP3S	Denial of Service Attack (POP3/POP3S)	"POP3PROXY DOS Attack Trap"	**Warning** When IronMail detects that the Denial of Service threshold has been reached via POP3 or POP3S connections, it can generate a warning alert.
POP3/POP3S	Password Cracking Attempt (POP3/POP3S)	"POP3PROXY Password Cracking Attempt Trap"	**Information** Whenever the Password Cracking threshold has been reached via POP3 or POP3S connections, an information alert can be generated.
IMAP4/IMAP4S	Denial of Service Attack (IMAP4/IMAP4S)	"IMAP4PROXY DOS Attack Trap"	**Warning** When IronMail detects that the Denial of Service threshold has been reached via SMTPI or SMTPIS connections, it can generate a warning.
IMAP4/IMAP4S	Password Cracking Attempt (IMAP4/IMAP4S)	"IMAP4PROXY Password Cracking Attempt Trap"	**Information** Whenever the Password Cracking threshold has been reached via IMAP4 or IMAP4S connections, an information alert can be generated.
Anti Virus Queue	Viruses Found	"AVQ Virus Found Intimation Trap"	**Information** Whenever a virus is detected in a message, an information alert can be generated.
Internal Queues	MIME Parsing Failure	"RIPQ MIME Parsing Failure Trap"	**Information** Whenever IronMail is unable to successfully “parse” or interpret a message’s MIME boundaries, an information alert can be generated.
Anomaly Detection	Anomaly Detection-IP Address	"ADE from same IP Trap"	**User-defined** You may set the alert level for the “messages from the same IP address” anomaly.
Anomaly Detection	Anomaly Detection-From Address	"ADE same From Address Trap"	**User-defined** You may set the alert level for the “messages from the same email address” anomaly.

Anomaly Detection	Anomaly Detection-Message Size	"ADE Same Message Size Trap"	**User-defined** You may set the alert level for the “messages are the same size” anomaly.
Anomaly Detection	Anomaly Detection-Message Subject	"ADE Same Message Subject Trap"	**User-defined** You may set the alert level for the “messages with the same subject line” anomaly.
Anomaly Detection	Anomaly Detection-Message Attachment	"ADE Same Attachment Trap"	**User-defined** You may set the alert level for the “messages have the same attachment” anomaly.
Anomaly Detection	Anomaly Detection-Attachment Extension	"ADE Same Attachment Extension Trap"	**User-defined** You may set the alert level for the “messages have the same attachment file extension” anomaly.
Anomaly Detection	Anomaly Detection-Virus	"ADE Same Virus Trap"	**User-defined** You may set the alert level for the “messages are infected with a virus” anomaly.
Anomaly Detection	Anomaly Detection-Same Virus	"ADE Same Unique Virus Trap"	**User-defined** You may set the alert level for the “messages are infected with the same virus” anomaly.
Anomaly Detection	Anomaly Detection Complex *Rule*	"ADE Complex Rule Trap"	**User Defined** You may set the aler level for alerts to be generated when a complex ADE rule is triggered.
License	Expiration 60 day warning	"60 Days License Notification"	**Information** IronMail will generate one information alert 60 days before a license is due to expire.
License	Expiration 30 day warning	"30 Days License Notification"	**Warning** IronMail will generate one warning alert 30 days before a license is due to expire.
License	Expiration 10 day warning	"Less than 10 Days License Notification"	**Critical** IronMail will begin generating daily alerts 10 days before a license is due to expire.

Virus Updates	Queue-Update Success	"AVQ Virus Update Completed Successfully"	**Information** IronMail will generate an information alert when a Sophos anti-virus update is downloaded and installed successfully.
Virus Updates	Queue-Update Failure	"AVQ Virus Update Failed"	**Notification** IronMail will generate a notification alert if a Sophos anti-virus update fails to download and install successfully.
Update	Failed	"UpdateFailed"	**Notification** If a *CMC* experiences a failed attempt to push a file update to a managed IronMail, it can generate a notification alert.
Update	Success	"Update Completed Successfully"	**Notification** When a CMC successfully pushes a file update to a managed IronMail, it can generate a notification alert.
Spam Queue	RBL Failure	"SPAM RBL Lookup Failure Trap"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	Reverse DNS Failure	"SPAM Reverse DNS Lookup Failure Trap"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	SLS Detected	"SLS Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	ESP Detected	"Enterprise Spam Profiler Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	System Defined Header Analysis Detected	"System Defined Header Analysis Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	End User Spam Reporting	"End User Spam Trap Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
Spam Queue	User Defined Header Analysis Detected	"User Defined Header Analysis Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information

Spam Queue	Enterprise Spam Reporting	"Enterprise Spam Trap Detected the Message as Spam"	For Log Actions - No alert; For Drop Action - Notification; For Other Actions - Information
SLS	Server Up	"SLS UP Trap"	**Notification** If IronMail restarts the SLS server, it can send a notification that the server is responding properly.
SLS	Server Down	"SLS DOWN Trap"	**Warning** If the SLS server shuts down, IronMail can send a warning.
SLS	Fallback Succeeded	"SLS Fallback was Successful"	**Notification** If SLS fallback is triggered and succeeds, IronMail can send a notification to that effect.
SLS	Fallback Failed	"SLS Fallback Attempt Failed"	**Warning** If SLS fallback fails, IronMail can send a warning.
CMC	Data Server Connectivity Error		**Restart** If CMC detects a connectivity error with the Data Server, it attempts to reestablish the connection.
CMC	Admin Server Connectivity Error		**Restart** If CMC detects a connectivity error with the Admin Server, it attempts to reestablish the connection.
SWM	Queue-Up	"SWMQ UP Trap"	**Notification** When IronMail restarts the SWM Queue, it can send a notification that the queue is responding properly.
SWM	Queue-Down	"SWMQ DOWN Trap"	**Error** If the SWM Queue shuts down, IronMail can send a warning.
SWM	Error	"SWMQ ERROR Trap"	**Warning/Error** If IronMail's SWM Queue experiences other errors, IronMail can generate either warning or error messages. (IronMail intelligently tracks persistent problems and escalates the alert message accordingly.)

SWM	Notification Failure	"SWMQ Notify Failure Trap"	**Notification** When the secure web delivery queue is unable to generate a notification, IronMail generates a notification.
IronWebMail	Up	"IWM UP Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Down	"IWM DOWN Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Error	"IWM ERROR Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Signature Attack	"IWM Signature Attack Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Buffer Overflow Attack	"IWM Buffer Overflow Attack Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Authentication Failed	"IWM Authentication Failed Trap"	**User Defined** You may set the alert type for this circumstance.
IronWebMail	Session Timed Out	"IWM Session Timeout Trap"	**User Defined** You may set the alert type for this circumstance.

Dropped Email Alerts

Note that if IronMail generates many alerts within a very brief period of time (e.g., 100 alerts within one minute), there is the potential that not all email alerts will successfully be sent to the administrator. If the internal mail server does not accept the “blast” of messages, undelivered alerts are dropped.

Importing MIBs

Before IronMail’s SNMP traps can provide all the available information to the SNMP service, two MIBs must be compiled within the SNMP application. Contact CipherTrust Support to request copies of these MIBS.

In addition to its own two MIB files, IronMail SNMP implementation requires the following MIBs to be installed on the SNMP server: IANAifType-MIB, IF-MIB, INET-ADDRESS, SNMP-FRAMEWORK, SNMPv2-CONF, SNMPv2-MIB, SNMPv2-SMI, and SNMPv2-TCI. Most SNMP software includes these MIBs.

The “Sensor ID” in the SNMP traps will report IronMail’s serial number (IronMail’s serial number may be viewed in the “About” dialog that is opened by clicking the “CipherTrust Info” hyperlink at the bottom of any IronMail page).

Note: When IronMail delivers any alert to an SNMP server, the SNMP console will receive it as a "Notification” alert. That is, even if the IronMail Administrator creates an SNMP alert mechanism for “Critical” alerts, they arrive at the SNMP console as “Notification” alerts. Administrators must create their own “hierarchy of criticality” for each of IronMail’s alerts on the SNMP console.

Reporting and Logging

Reports and Log Files

IronMail can generate daily reports in HTML format showing detailed information about the messages it processes each day. Additionally, the reports may be archived as “CSV” (comma separated values) files, for analysis in third-party applications.

While Reports provide a “high level” overview of IronMail’s message-processing activity, Logs show “low level”—or detailed—information about message processing at the level of the individual message. Depending on the logging level configured for each IronMail subsystem, the logs will report on the specific steps it took when processing individual messages. While logs are used primarily by CipherTrust Support engineers for troubleshooting purposes, administrators are well advised to become familiar with them as well. (Summary logs can also be exported in "real time" as SysLogs.)

All messages that IronMail processes (with the exception of messages IronMail drops because of an email policy’s action) may be saved to disk and archived.

IronMail generates its Reports and Logs (if the process is running) and archives messages at approximately 3:30 AM each morning. Note that because IronMail generates the log files the next day, the files’ date will be offset from the date of the actual data by one day.

The Reports/Log Files hyperlink in the left navigation frame of the Web Administration interface expands to offer Reports Configuration, Reports, CSV Reports, SysLog Configuration, Detailed Logs, Summary Logs, and Archive sub-menus.

IronMail Reports

Reports

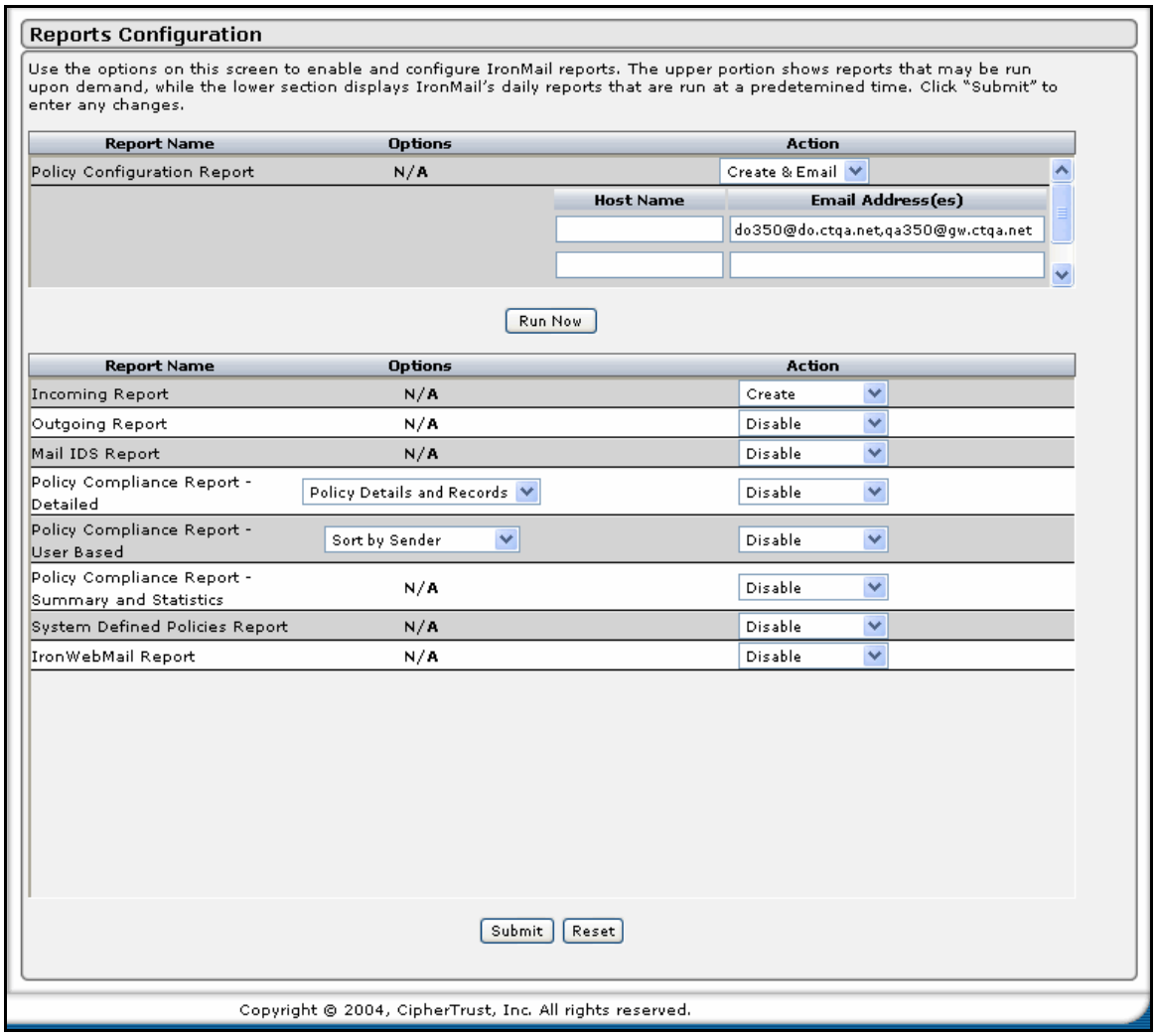
IronMail generates a variety of reports informing the Administrator of all of IronMail’s activity. The reports cover two broad categories: the email that IronMail processes, and IronMail’s internal activity.

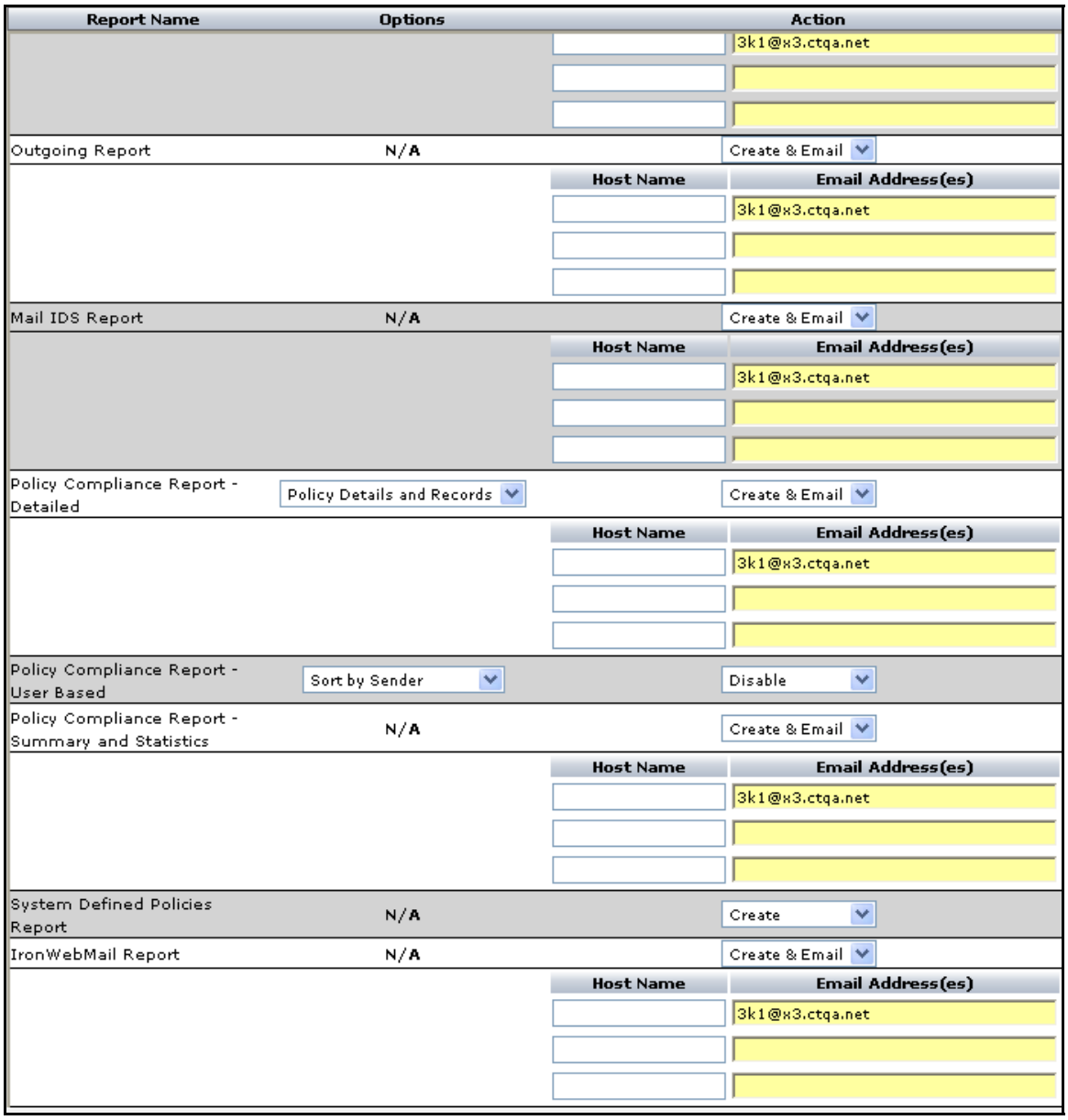
Email activity can be viewed either as summaries or as detailed reports. The summaries show the top senders and receivers during a 24 hours period, who sent or received the most mail by volume (in megabytes), who sent or received the most encrypted messages, etc. Of particular interest to administrators is the summary report that provides spam statistics needed for decisions in a concise and easily understandable form.

All reports will be automatically sent to the recipient or recipients whose email addresses are specified if IronMail is configured to do so. In addition, IronMail will generate, “on demand,” a report detailing every email *policy* that has been created. That is, you can view which Content Filtering “dictionaries” have been created and are in use, to whom Mail Monitoring policies have been applied, etc.

Reports Configuration

IronMail can generate a variety of daily reports, but only if configured to do so.


Reports Configuration
Use the options on this screen to enable and configure IronMail reports. The upper portion shows reports that may be run upon demand, while the lower section displays IronMail's daily reports that are run at a predetermined time. Click "Submit" to enter any changes.
Report Name
Options
Action
Policy Configuration Report
N/A
Create & Email
Host Name
Email Address(es)
do350@do.ctqa.net,qa350@gw.ctqa.net
Run Now
Report Name
Options
Action
Incoming Report
N/A
Create
Outgoing Report
N/A
Disable
Mail IDS Report
N/A
Disable
Policy Compliance Report - Detailed
Policy Details and Records
Disable
Policy Compliance Report - User Based
Sort by Sender
Disable
Policy Compliance Report - Summary and Statistics
N/A
Disable
System Defined Policies Report
N/A
Disable
IronWebMail Report
N/A
Disable
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.



The HTML Reports Configuration table lists all reports that can be created, and allows the following options:

Report Name	All reports that IronMail can generate are identified: • **Incoming Report:** In addition to reporting daily totals and averages, the Incoming Report is like a "top 10" list—reporting the top ten users who send messages with or without *SSL*, and their volume, both in terms of message count and MB. The Incoming Report also identifies the top 10 file *attachment types*. (The Content Filtering Queue must be enabled, running, and enforcing at least one *policy* in order for this report to identify the top 10 file types.) **Note:** The totals reported in the Incoming Report are based on messages received, regardless of the number of domains to which they are addressed. Each message is counted once, even if it is addressed to multiple recipients. • **IronWebMail Report:** The IronWebMail Report reports IronWebMail's

	session totals and averages, session counts, connection denials, and login features. • **Mail IDS Report:** The Mail-IDS Report shows the results of IronMail's Mail-IDS monitoring and activity: password strength, denial of service protection, password cracking, program and filesystem integrity, and IDS alerts. • **Outgoing Report:** Similar to the Incoming Report, the Outgoing Report is like a "top 10" list showing statistics about messages that internal users deliver outbound. The Outgoing Report also identifies the top 10 file *attachment types*. (The Content Filtering Queue must be enabled, running, and enforcing at least one policy in order for this report to identify the top 10 file types.) **Note:** The totals reported by the Outgoing Report are based on the domains to which messages are addressed. Any message addressed to more than one recipient *in more than one domain* will be counted multiple times (once for each domain). • **Policy Compliance-Detailed:** The detailed Policy Compliance Report shows every action that IronMail executed on a message because of an email policy. (The Policy Compliance Report is a very useful resource when implementing spam and email policies. It may assist administrators in identifying how effective a particular policy is, or is not, in performing its intended function.) **Note:** The Policy Compliance-Detailed report may be configured using the pick list to generate policy details only or both policy details and records. • **Policy Compliance-Summary and Statistics:** The summary Policy Compliance Report shows the top 20 email policies that IronMail enforced, and the users who were affected. **Note:** The values in % Detected in Total in the Spam Summary section of this report may appear misleading if the user does not understand how they are calculated. The percentages are calculated as follows: (messages detected by the tool / total *spam* messages) * 100 = % If the user totals all the percentages in the Spam Summary section, the total may exceed 100%. The same message may be detected by more than one tool, resulting in its appearance in multiple totals and percentages. **Note:** The Administrator should not expect the total number of messages shown in the Summary report to represent a sum of the totals from the Incoming Report and the Outgoing Report. As shown above, these two reports count different entities. The Incoming Report counts individual messages, no matter how many domains or recipients are included; one message addressed to three recipients, for example, will still count only once. The Outgoing Report counts domains to which messages are addressed; for example, one message sent to five domains will be counted five times. The likelihood that Total Incoming + Total Outgoing = Total Messages is, at best, very remote. The two are not really connected. • **Policy Compliance-User-based:** the user-based Policy Compliance Reports shows the results of IronMail's enforcement of email policies, but sorts the results by individual user. **Note:** The User report does not include results from Deny Lists. Those results appear only in the Policy Compliance Report - Detailed.
Sort By	The "Sort By" column is only enabled for the Policy Compliance—User-based

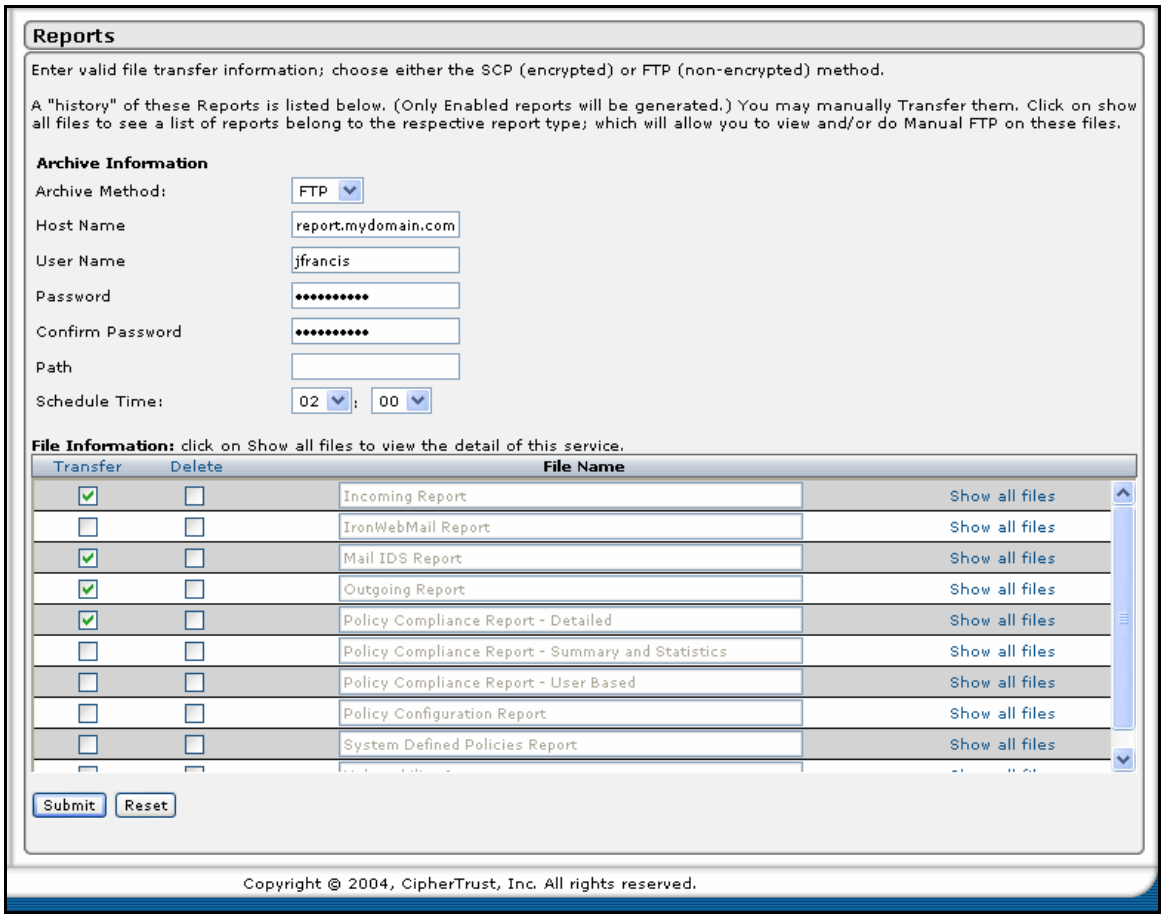
	report. The Policy Compliance report's data may be sorted by: • message sender • message receiver • the internal user.
Action	The Action pick list offers three options: • **Disable:** When disabled, the report is not generated. • **Create:** When selected, IronMail generates the report but does not automatically send it by email. The report may be viewed in the Web Administration interface, and may automatically and/or manually be transferred to an archive server via the SCP or FTP protocols. • **Create and Email:** When selected, IronMail generates the report and emails it to specified users. The report may also be viewed within the Web Administration interface, and may automatically and/or manually be transferred to an archive server via the SCP or FTP protocols.
Host Name	Enter the host name or the IP address of the server to which the reports are to be sent.
Email Address(es)	The **Email Address(es)** input field is disabled unless **Create and Email** was selected in the Action column. Multiple email addresses may be entered, with each address separated by a comma. (Do not enter spaces between commas and subsequent email addresses.)

Above the table of regular Daily Reports is an option to create or create and email a Policy Configuration Report. The report details every email policy configured on the IronMail appliance. Select the option to "create" or "create and email," and if the report is to be emailed, provide a valid host name or email address in the input field. Click **Run Now** to generate the report. Within a few moments, the report will be available in the *Monitoring > Reports/Log Files > Reports* window.

The Policy Configuration report allows the Administrator to easily review all IronMail policy settings without having to navigate through the graphical user interface to retrieve the same information.

HTML Reports

IronMail creates a variety of HTML reports viewable within a browser window, or that may be archived to disk. IronMail generates the daily reports at approximately 3:30 AM each day, and when the reports are generated, they contain the previous 24 hours' worth of data.


Reports
Enter valid file transfer information; choose either the SCP (encrypted) or FTP (non-encrypted) method.
A "history" of these Reports is listed below. (Only Enabled reports will be generated.) You may manually Transfer them. Click on show all files to see a list of reports belong to the respective report type; which will allow you to view and/or do Manual FTP on these files.
Archive Information
Archive Method: FTP
Host Name report.mydomain.com
User Name jfrancis
Password
Confirm Password
Path
Schedule Time: 02 : 00
File Information: click on Show all files to view the detail of this service.
Transfer
Delete
File Name
Incoming Report
IronWebMail Report
Mail IDS Report
Outgoing Report
Policy Compliance Report - Detailed
Policy Compliance Report - Summary and Statistics
Policy Compliance Report - User Based
Policy Configuration Report
System Defined Policies Report
Show all files
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

Daily Reports may be archived automatically on a user-defined schedule. Provide the following archive information:

Archive Method	Select an archive method IronMail should use when transferring the Reports: • **SCP:** Select SCP to transfer the file securely using the SCP *protocol*. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the filename.
Host Name	Enter the host name of the archive server.
Username	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.
Path	Enter the path string to the location on the archive server where IronMail should transfer the Reports. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.

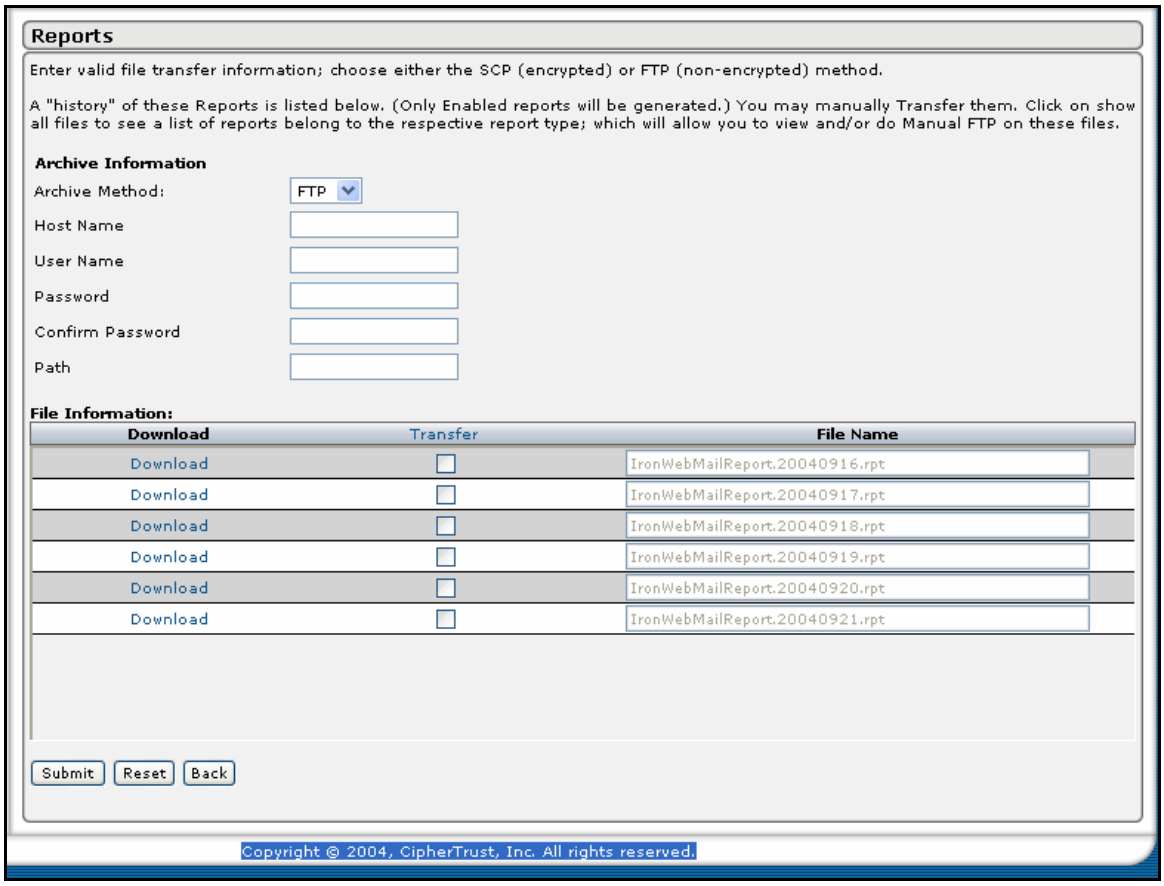
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the Reports. It is recommended that administrators choose a transfer time after 4 AM to allow enough time for the reports to run and rollover the previous days logs.

The table of Reports displays the following:

Transfer	A **Transfer** check box allows the selection of Daily Reports to be automatically transferred to the archive server at the specified hour. Reports that are not selected in this column are not transferred.
Delete	A **Delete** check box allows the automatic deletion of selected Reports after they have been transferred. If the **Delete** check box is not selected, the Daily Report remains on IronMail's hard disk until its Cleanup Schedule deletes old data files. ***IronMail does not confirm whether or not a file transfer was successful.*** *If the* **Delete** *check box is selected, IronMail will delete the Report after it has attempted to transfer the file, whether the transfer was successful or not.*
File Name	The names of the available reports are listed in this column: • **Incoming Report:** In addition to reporting daily totals and averages, the Incoming Report is like a "top 10" list—reporting the top ten users who send messages with or without *SSL*, and their volume, both in terms of message count and MB. The Incoming Report also identifies the top 10 file attachment types. (The Content Filtering Queue must be enabled, running, and enforcing at least one *policy* in order for this report to identify the top 10 file types.) • **IronWebMail Report:** The IronWebMail Report reports IronWebMail's session totals and averages, session counts, connection denials, and *login features.* • **Mail IDS Report:** The Mail-IDS Report shows the results of IronMail's Mail-IDS monitoring and activity: password strength, denial of service protection, password cracking, program and filesystem integrity, and IDS alerts. • **Outgoing Report:** Similar to the Incoming Report, the Outgoing Report is like a "top 10" list showing statistics about messages that internal users deliver outbound. The Outgoing Report also identifies the top 10 file attachment types. (The Content Filtering Queue must be enabled, running, and enforcing at least one policy in order for this report to identify the top 10 file types.) *Note that messages missing an RFC821 From address will display as **Unknown**.* • **Policy Compliance-Detailed:** The detailed Policy Compliance Report shows every action that IronMail executed on a message because of en email policy. (The Policy Compliance Report is a very useful resource when implementing spam and email policies. It may assist administrators in identifying how a particular policy is, or is not, effective in performing its intended function.) • **Policy Compliance-Summary and Statistics:** The summary Policy Compliance Report shows the top 20 email policies that IronMail enforced, and the users who were affected. • **Policy Compliance-User-based:** the user-based Policy Compliance Reports shows the results of IronMail's enforcement of email policies, but sorts the results by the individual users affected by the policies. • **Policy Configuration:** the Policy Configuration Report shows a detailed listing of all rules that have been created, sorted by functional area. This report is not generated on a daily basis as are the other IronMail reports, but may be run at the user's discretion from the Reports screen.

	• **System-Defined Policy:** the system-defined policy report shows the currently enabled system-defined policies and the results of their enforcement. Policies are sorted by functional area (e.g., ESP, ADE, etc.). • **Vulnerability Assessment:** the Vulnerability Assessment Report is not a scheduled report. It can be run from the Vulnerability Assessment screen. Vulnerability Assessment applies to a single IP address; the report shows the results of the assessment. When IronMail reports statistics about the number of messages it processed, and which messages were affected by an email policy, there may be discrepancies between the total count and sub-total counts of messages in IronMail's Daily Reports. This is because IronMail's Queue Services do not necessarily examine every message. For example, if the Content Filtering Queue was the first to examine a message, and sent the message to a quarantine queue as a result of the policy, the message might never be examined by the Anti-Spam Queue. Or if the Content Filtering Queue notes that a message contains a large number of file attachments and the message is ultimately dropped, those attachment file-types may not be represented in IronMail's SMTPO Outgoing Daily Report. The result of enforced email policies, and the order in which IronMail's Queue Services process messages, all impact the data recorded in IronMail's Daily Reports.
Show all files	The **Show all files** hyperlink opens a secondary browser window displaying the names of previous days' Reports that have not yet been deleted by IronMail's Cleanup Schedule. Note that each Report contains a date suffix in YYYYMMDD format. Administrators may manually view, transfer, or delete individual Reports from within this secondary window.

Clicking the Show All Files link opens a screen like the one below, showing all available versions by date of the specific report.



Spam Summary Report

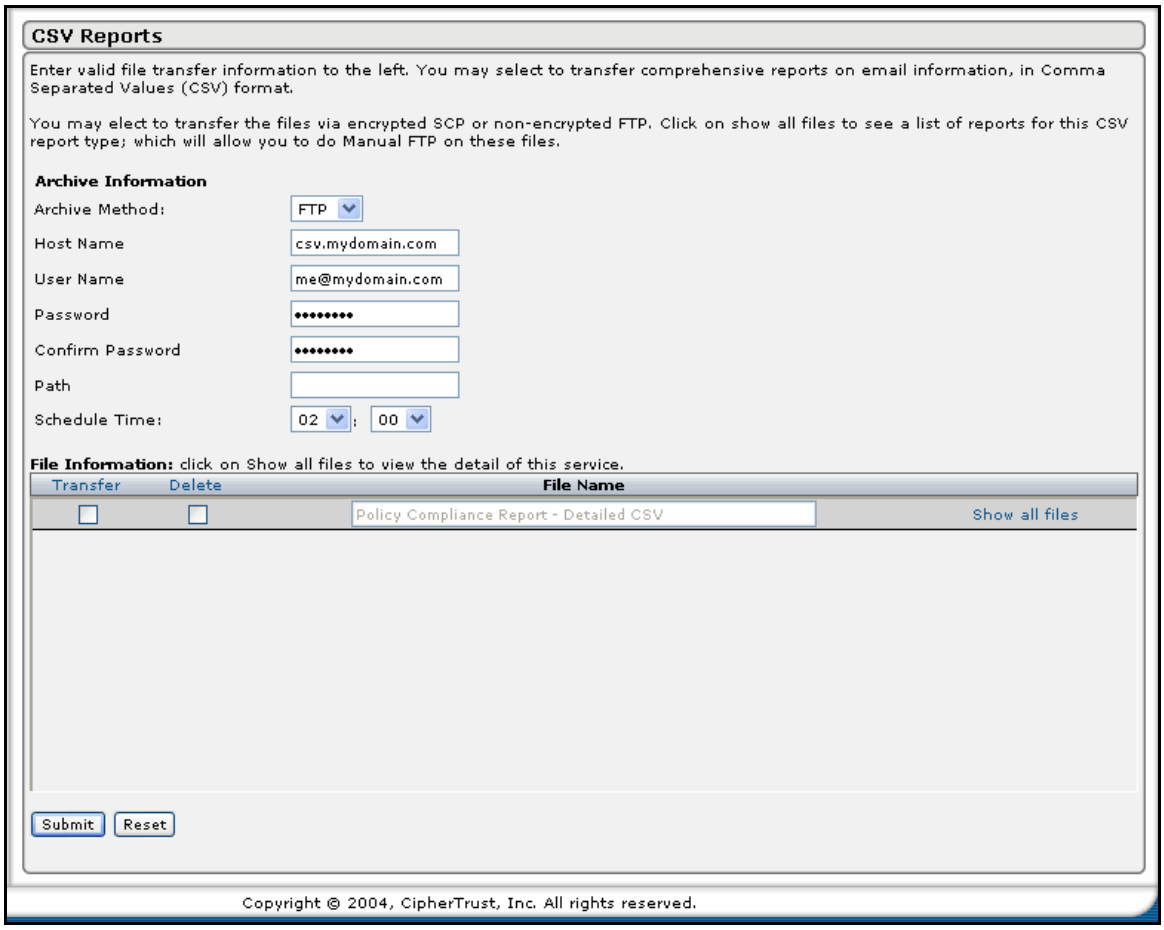
This report is a simplified standard report that provides more easily readable spam statistics. The Anti-Spam Summary simplifies data-gathering and provides essential information for decision making.

The report provides the total incoming emails, and then the relevant totals from the *Policy* Compliance Detailed Report (just the totals). These statistics include information like: total hits for RDNS, total hits for RBL, totals for ESP, SLS, SDHA, UDHA, etc., and total hits for all tools combined. Action totals are also included, such as: total messages logged as spam, total messages quarantined as spam, total messages dropped as spam, etc. - one total for each action. The percentage of inbound email caught as spam is calculated as well.

CSV Reports

IronMail can generate a daily comma separated values-formatted (CSV) text file that records the From, To, Size, Date, Time, and every action IronMail performed on every message processed that day. (Whereas the daily Incoming and Outgoing Reports only show “totals” and “top 10’s” for each day, this report lists every single email that was processed. Note that this file is a “data dump” showing every action IronMail took on a message—whether actions were taken because of an email *policy*, or if messages were delivered with no action taken. Because this file contains so much data, CSV files can easily reach 50-100MB in size in high mail-volume environments. Administrators are cautioned, therefore, to configure the cleanup schedule for “Log Files” data so that these files do not remain on IronMail’s disk longer than three or four days (See *System > Cleanup Schedule > “Reports data”*).

Policy Compliance Report - Detailed must be enabled before you can configure and generate the CSV reports. The following screen allows you to configure the reports.


CSV Reports
Enter valid file transfer information to the left. You may select to transfer comprehensive reports on email information, in Comma Separated Values (CSV) format.
You may elect to transfer the files via encrypted SCP or non-encrypted FTP. Click on show all files to see a list of reports for this CSV report type; which will allow you to do Manual FTP on these files.
Archive Information
Archive Method:
FTP
Host Name
csv.mydomain.com
User Name
me@mydomain.com
Password
Confirm Password
Path
Schedule Time:
02
00
File Information: click on Show all files to view the detail of this service.
Transfer
Delete
File Name
Policy Compliance Report - Detailed CSV
Show all files
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

IronMail can transfer CSV files to an archive server, either manually or automatically. If archive server information is provided in the six **Archive Information** input fields at the top of the page and the **Transfer** check box is selected in the table below, IronMail will automatically transfer the file at the specified hour. When the **Archive Information** input fields are left blank, or if the **Transfer** check box is de-selected in the table below, CSV Reports may be manually transferred by entering archive server information in the secondary browser window that opens after clicking the **Show all files** hyperlink.

The automatic transfer of CSV files requires the following user input:

Archive Method	Select an archive method IronMail should use when transferring the CSV files: • **SCP:** Select SCP to transfer the files securely using the SCP *protocol*. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the files in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files to the same directory, the *host name* is appended to the file name during the transfer.
Host Name	Enter the host name of the archive server.
Username	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.

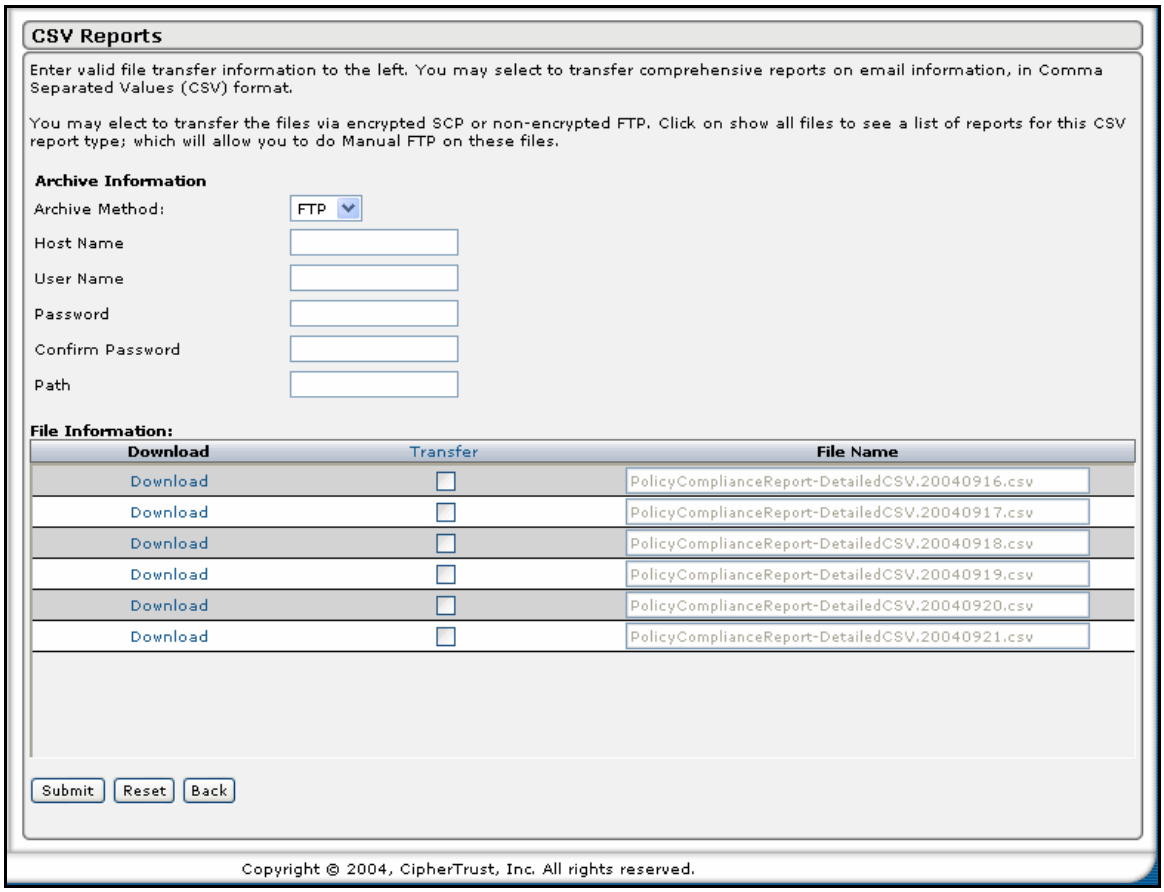
Path	Enter the path string to the location on the archive server where IronMail should transfer the files. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule	Time Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the files.

To configure IronMail for manual CSV file delivery only, do not enter file transfer information on this page. For manual file transfer, enter the file transfer information in the secondary browser window that opens after clicking the **Show all files** hyperlink in the table of files below.

Below the **Archive Information** input fields is a one-row table offering the following information and actions:

Transfer	If the **Transfer** check box is selected and Archive Information is provided in the input fields above, IronMail will automatically transfer the CSV file at the scheduled hour. Click **Submit** after selecting **Transfer** to save the user input.
Delete	Select the **Delete** check box and click **Submit** to delete the most recent (yesterday's) CSV file.
File Name	This column identifies the name of the most recent file. (Note that because IronMail generates these files at approximately 12:30 AM, each day's CSV data does not become available until the next morning.
Show all files	The **Show all files** hyperlink opens a secondary browser window that displays all CSV files that IronMail's Cleanup Schedule has not yet deleted from disk. (Note that each file name includes the date that the file was generated.)

When the **Show all files** hyperlink is clicked, a window opens, displaying any CSV files that have not yet been deleted by IronMail's Cleanup Schedule. Enter Archive Information in the six input fields at the top of the window, and select the **Download** or **Transfer** check boxes for specific files.



Understanding the CSV File

The contents of the CSV file is a raw "data dump" from IronMail's database. When IronMail queries the database, and the database returns its data, the raw data is not returned in any specific order. Message ID numbers and dates, for example, do not follow each other sequentially. The only "order" implicate in the file is that all data is grouped according to one of four types of information: Message information, Domain information, *Policy* information, and Message Part information.

IronMail presents, in "pieces," information about how it processed each individual messages. In some cases, IronMail will only present just one "piece" of information because that is all there is to report, and that information will be displayed in a single line in the CSV file. In other cases, IronMail may report multiple pieces of information, with each "piece" appearing on separate lines of the file. Once the file is imported into a third-party application, use the application's tools to sort or "order" the data so that all the pieces of the message are grouped together.

The data in the CSV file contains up to ten **comma-separated fields on each row or line**. (Depending on the amount of data in a line, and the application in which the data is being viewed, message data may wrap to a second line.)

```
3,18,0,1004,{'q_id': '6'\, 'msg_text': 'The IronMail(TM) Quarantine Viewer moved the message as requested in the UI.'\, 'msg_subject': 'Quarantine Viewer moved message'},2003-02-05 14:17:07
```

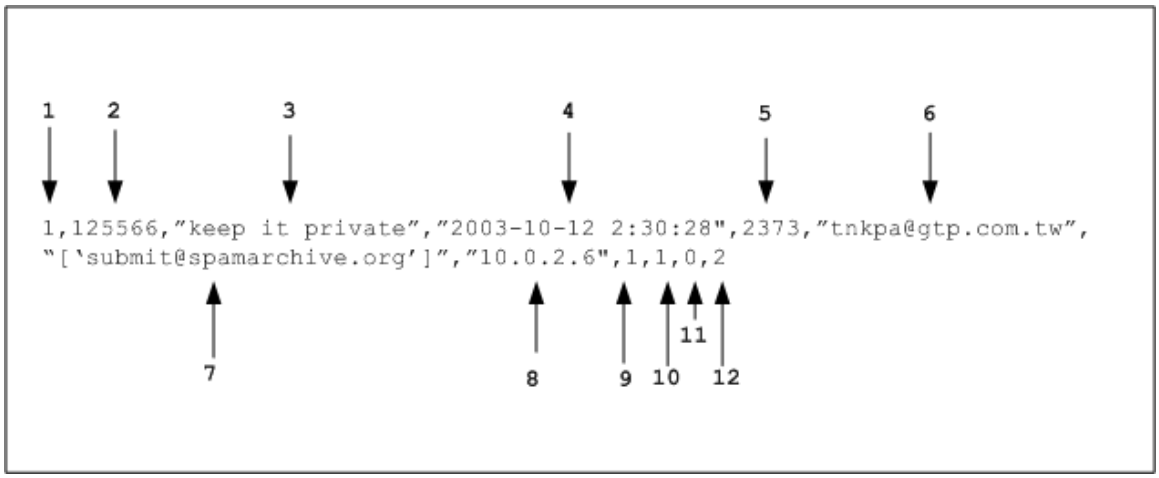
The **first field** represents what kind of information is displayed on that row. One of three values will appear:

- 1 = Message information
- 2 = Domain information

- 3 = Policy information
- 4 = Message part information

The remaining fields on each row differ, depending on the type of information being displayed.

Message Information:



The **first field** indicates the information type. Each row of Message information begins with the numeral "1."

The **second field** is the "message ID"—a number that uniquely identifies the message. The message ID is a critical piece of information, allowing administrators to identify and track a single message in all of IronMail's logs.

The **third field** is the message's Subject, reported in its entirety.

The **fourth field** is the message's date—the timestamp when IronMail received the message.

The **fifth field** is the message's size in bytes.

The **sixth field** is the Mail From address—from whom the message originated.

The **seventh field** is the list of Recipient addresses—to whom the message was addressed.

The **eighth field** is the source IP address—the *IP address* of the message sender.

The **ninth** field is the Message direction. One of these values will appear:

- 0 = Inbound
- 1 = Outbound

The **tenth** field identifies the internal user. One of these values will appear:

- 0 = Sender
- 1 = Recipient

The **eleventh** field identifies the message type, to indicate if the message was received by SMTP Proxy using TLS (*SSL*). One of these Message Type values will appear:

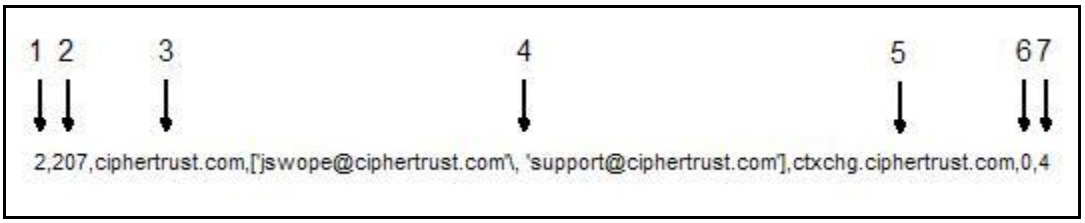
- MSG_TYPE_NORMAL = 0
- MSG_TYPE_NOTIFICATION = 1
- MSG_TYPE_FORWARDED = 2

- MSG_TYPE COPIED = 3
- MSG_TYPE_DSN = 4
- MSG_TYPE_SWM = 5
- MSG_TYPE_REPORTS = 6
- MSG_TYPE_EUSR_OUT = 7
- MSG_TYPE_EST_OUT = 8
- MSG_TYPE_EUSR_IN = 9
- MSG_TYPE_EST_IN = 10
- MSG_TYPE_SECURE = 11
- MSG_TYPE_FWD_ATTACH = 12

The **twelfth** field indicates if the messages was encrypted or signed. One of these values will appear:

- 0 = Unsigned
- 1 = Signed
- 2 = Encrypted
- 3 = Decrypted

Domain Information:



The **first field** indicates the information type. Each row of Domain information begins with the numeral "2."

The **second field** is the "message ID"—a number that uniquely identifies the message. The message ID is a critical piece of information, allowing administrators to identify and track a single message in all of IronMail's logs. Note that though message IDs may look like they are grouped serially, there is no IronMail requirement that they are sorted in this CSV file.

The **third field** is the recipient's domain.

The **fourth field** identifies the recipient(s) of the message.

The **fifth field** identifies the internal host to which the message was delivered.

The **sixth field** identifies the "delivery mode"—one of six values will appear:

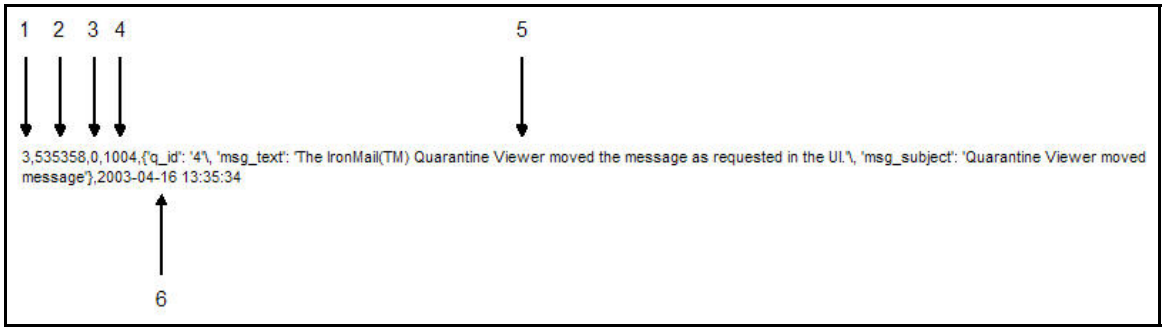
- 0 = Normal, plain-text message
- 1 = TLS delivery
- 2 = S/*MIME* delivery
- 3 = PGP delivery
- 4 = SWM (Secure Web Delivery) delivery

- 5 = TLS deny (A TLS delivery was attempted, but an IronMail policy denying TLS for that user forced the message to be delivered in plain-text.)

The **seventh field** describes the message's status, and will display one of four values:

- -1 = Not yet picked up for delivery (The message was deleted by the SMTPO Service, or it is in the Quarantine Queue because of a failed delivery attempt or other IronMail policy.)
- 0 = Picked
- 1 = Connected
- 2 = Transmitted
- 4 = Delivered
- 5 = Undeliverable dropped
- 7 = UI Dropped (The message was dropped by the web administrator.)
- 8 = SWM (Secure Web Delivery) delivery

Policy Information:


1 2 3 4
5
3,535358,0,1004,{'q_id': '4'\, 'msg_text': 'The IronMail(TM) Quarantine Viewer moved the message as requested in the UI.'\, 'msg_subject': 'Quarantine Viewer moved message'},2003-04-16 13:35:34
6

The **first field** indicates the information type. Each row of Policy information begins with the numeral "3."

The **second field** is the "message ID"—a number that uniquely identifies the message. The message ID is a critical piece of information, allowing administrators to identify and track a single message in all of IronMail's logs. Note that though message IDs may look like they are grouped serially, there is no IronMail requirement that they are sorted in this CSV file.

The **third field** identifies a message's "part" number. This field reports a numeric value representing which part of the message is being described. (Messages can have many MIME parts—IronMail defaults to only accepting messages that contain less than 1,000 parts.) A "0" in this field represents "the whole message." Any other value is the part number. Note that a message's parts are not necessarily grouped together in the CSV file—a third party utility is required to group all message parts by their ID number, and then sort them in ascending or descending order.

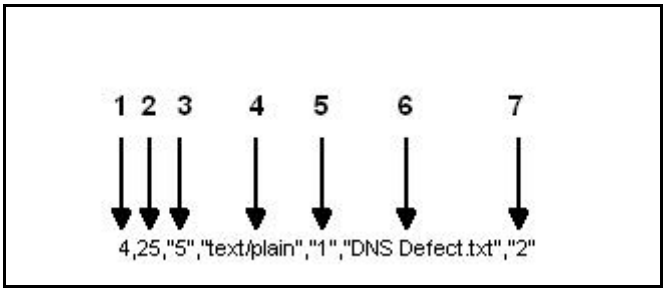
The **fourth field** is a number that identifies each possible IronMail action. (This number is used internally by IronMail, but corresponds to the actions that IronMail's policies enforce. View the table of actions.)

The **fifth field** may or may not be present, depending on the policy IronMail enforced. For example, a policy with a "quarantine action" requires a number as an "action value" indicating how many days a message is to be quarantined, and a policy with a "drop action" may have a text message (replacing the dropped message part) as an "action value." (Note that "text" action values may be lengthy, and force the row in the CSV file to wrap to additional lines.) Depending on the action,

the fifth field may contain numerous data elements that describe the totality of the action, e.g., message Subject, Recipient address, or timestamp.

The **sixth field** is the timestamp of the action—the time the action occurred.

Message Part Information



The **first field** indicates the information type. Each row of Message Part information begins with the numeral "4."

The **second field** is the "message ID"—a number that uniquely identifies the message. The message ID is a critical piece of information, allowing administrators to identify and track a single message in all of IronMail's logs. Note that though message IDs may look like they are grouped serially, there is no IronMail requirement that they are sorted in this CSV file.

The **third field** identifies a message's "part" number. This field reports a numeric value representing which part of the message is being described. (Messages can have many MIME parts—IronMail defaults to only accepting messages that contain less than 1,000 parts.) A "0" in this field represents "the whole message." Any other value is the part number. Note that a message's parts are not necessarily grouped together in the CSV file—a third party utility is required to group all message parts by their ID number, and then sort them in ascending or descending order.

The **fourth field** identifies the message content type.

The **fifth field** identifies if the part is an attachment or the message body. One of two values will appear:

- 0 = Attachment
- 1 = Body

The **sixth field** identifies the attachment name.

The **seventh field** describes the part format as identified by the Content Extraction Engine**.**

Action Codes

The fourth field in the *Policy* Information lines contains a numeric value that identifies the action IronMail performed on a message. (The "action" also implies the Queue service where the action occurred.) The table below provides a "map" for all IronMail'sactions.

Action Code Number	Description
Mail Monitoring Policies	
101	'Subject rewritten based on recipient domain'
102	'Blind copy based on recipient domain'
103	'Forward as attachment based on recipient domain'
104	'Quarantined based on recipient domain'
105	'Dropped based on recipient domain'
106	'Message re-routed based on recipient domain'
107	'Log only based on recipient domain'
108	'Subject rewritten based on message subject'
109	'Blind copy based on subject'
110	'Forward as attachment based on subject'
111	'Quarantined based on subject'
112	'Dropped based on subject'
113	'Message re-routed based on subject'
114	'Log only based on subject'
115	'Subject rewritten based on sender group'
116	'Copied based on sending group'
117	'Forward as attachment based on sender group'
118	'Quarantined based on sender group'
119	'Dropped based on sender group'
120	'Message re-routed based on sender group'
121	'Log only based on sender group'

122	'Subject rewritten based on sender'
123	'Copied based on sender'
124	'Forward as attachment based on sender'
125	'Quarantined based on sender'
126	'Dropped based on sender'
127	'Message re-routed based on sender'
128	'Log only based on sender'
129	'Subject rewritten based on sender domain '
130	'Copied based on sender domain'
131	'Forward as attachment based on sender domain'
132	'Quarantined based on sender domain'
133	'Dropped based on sender domain'
134	'Message re-routed based on sender domain'
135	'Log only based on sender domain'
136	'Subject rewritten based on recipient group'
137	'Copied based on recipient group'
138	'Forward as attachment based on recipient group'
139	'Quarantined based on recipient group'
140	'Dropped based on recipient group'
141	'Message re-routed based on recipient group'
142	'Log only based on recipient group'
143	'Subject rewritten based on recipient'
144	'Copied based on recipient'
145	'Forward as attachment based on recipient'

146	'Quarantined based on recipient'
147	'Dropped based on recipient'
148	'Message re-routed based on recipient'
149	'Log only based on recipient'
150	'Secure Delivery based on recipient'
151	'Secure Delivery based on the sender'
152	'Secure Delivery based on the recipient domain'
153	'Secure Delivery based on the sender domain'
154	'Secure Delivery based on the recipient group'
155	'Secure Delivery based on the sender group'
156	'Secure Delivery based on the subject'
157	'Forward based on recipient'
158	'Forward based on the sender'
159	'Forward based on the recipient domain'
160	'Forward based on the sender domain'
161	'Forward based on the recipient group'
162	'Forward based on the sender group'
163	'Forward based on the subject'
164	'Copy as an attachment based on recipient'
165	'Copy as an attachment based on sender'
166	'Copy as an attachment based on recipient domain'
167	'Copy as an attachment based on sender domain'
168	'Copy as an attachment based on recipient group'
169	'Copy as an attachment based on sender group'

170	'Copy as an attachment based on subject'
Encrypted Message Filtering Policy	
201	'Encrypted message dropped based on sender'
202	'Plain message dropped based on sender'
203	'Encrypted message dropped based on recipient'
204	'Plain message dropped based on recipient'
205	'Encrypted message dropped based on sending group'
206	'Plain message dropped based on sending group'
207	'Encrypted message dropped based on recipient group'
208	'Plain message dropped based on recipient group'
209	'Encrypted message dropped based on recipient domain'
210	'Plain message dropped based on recipient domain'
211	'Encrypted message dropped based on sending domain'
212	'Plain message dropped based on sending domain'
213	'Encrypted message quarantined based on sender'
214	'Plain message quarantined based on sender'
215	'Encrypted message quarantined based on recipient'
216	'Plain message quarantined based on recipient'
217	'Encrypted message quarantined based on sending group'
218	'Plain message quarantined based on sending group'
219	'Encrypted message quarantined based on recipient group'
220	'Plain message quarantined based on recipient group'
221	'Encrypted message quarantined based on recipient domain'
222	'Plain message quarantined based on recipient domain'

223	'Encrypted message quarantined based on sending domain'
224	'Plain message quarantined based on sending domain'
225	'Encrypted message allowed based on sender'
226	'Plain message allowed based on sender'
227	'Encrypted message allowed based on recipient'
228	'Plain message allowed based on recipient'
229	'Encrypted message allowed based on sending group'
230	'Plain message allowed based on sending group'
231	'Encrypted message allowed based on recipient group'
232	'Plain message allowed based on recipient group'
233	'Encrypted message allowed based on recipient domain'
234	'Plain message allowed based on recipient domain'
235	'Encrypted message allowed based on sending domain'
236	'Plain message allowed based on sending domain'
Attachment Filtering Policies	
301	'Message Copied Attachment Filtering'
302	'Attachment renamed'
303	'Attachment dropped'
304	'Message forwarded as attachment Filtering'
305	'Attachment quarantined'
306	'Message re-routed Attachment Filtering'
307	'Log Attachment'
308	'Subject rewritten Attachment Filtering'
309	'Message Dropped'

310	'Secure delivery of Message '
311	'Action pass through for attachment'
312	'Message copied as an attachment'
Content Filtering Policies	
401	'Message Copied Content Filtering'
402	'Filtered words replaced with text string'
403	'Filtered words prefixed with text string'
404	'Messages with dropped parts Content Filtering'
405	'Messages that were forwarded as attachment Content Filtering'
406	'Message Quarantined Content Filtering'
407	'Messages that were dropped Content Filtering'
408	'Message re-routed based on '
409	'Log Dictionary'
410	'Secure Delivery for Dictionary'
411	Message copied as an attachment
Message Stamping Policy	
501	'Messages that were Stamped'
Off Hour Delivery Policy	
601	'Messages delayed to Off-Hour Delivery time'
IronMail Notifications Delivered	

602	'Notification message generated by IronMail';
Virus Queue Actions	
701	'No action was taken by Virus Scan Queue'
702	'Messages dropped by Virus Scan Queue'
703	'Extension changed by Virus Scan Queue'
704	Not in use ('This part dropped by Virus Scan Queue
705	'Messages repackaged by Virus Scan Queue'
706	'Virus Cleaned by Virus Scan Queue'
707	'Neglecting sweep errors by Virus Scan Queue'
708	*Not in use* ('This part is dropped by Virus Scan Queue')
709	'The message is quarantined by Virus Scan Queue'
710	'A virus was detected'
711	'Sweep errors detected.'
712	'File encryption (password protection) detected.'
713	'Extension changed for sweep errors'
714	'Extension changed for file encryption (password protection)'
715	'Extension override for generic scan error - message passed through Virus Scan Queue'
Rip Queue Actions	
801	'Message dropped by Rip Queue because it was unable to parse it'
802	*Not in use* ('Message repackaged by Rip Queue because it was unable to parse it')
803	'Message quarantined by Rip Queue because it was unable to parse it'
804	'Message dropped by Rip Queue because a mail loop was detected'
805	'Message quarantined by Rip Queue because a mail loop was detected'

806	' *MIME* parse failed. Message delivered to recipient after it parses through all configured queues except Content Filtering Queue'
807	'MIME parse failed. Message delivered to alternate address after it parses through all configured queues except Content Filtering Queue'
Spam Queue Policies	
901	'Message dropped by Anti-Spam RBL'
902	'Message subject rewritten by Anti-Spam RBL'
903	'Message quarantined by Anti-Spam RBL'
904	'Message logged by Anti-Spam RBL'
905	'New header added by Anti-Spam RBL'
906	'Message copied by Anti-Spam RBL'
907	'Message forwarded by Anti-Spam RBL'
911	'Message dropped by Anti-Spam RDNS'
912	'Message subject rewritten by Anti-Spam RDNS'
913	'Message quarantined by Anti-Spam RDNS'
914	'Message logged by Anti-Spam RDNS'
915	'New header added by Anti-Spam RDNS'
916	'Message copied by Anti-Spam RDNS'
917	'Message forwarded by Anti-Spam RDNS'
921	'Message dropped by Anti-Spam SLS'
922	'Message subject rewritten by Anti-Spam SLS'
923	'Message quarantined by Anti-Spam SLS'
924	'Message logged by Anti-Spam SLS'
925	'New header added by Anti-Spam SLS'

926	'Message copied by Anti-Spam SLS'
927	'Message forwarded by Anti-Spam SLS'
941	'Message dropped by Anti-Spam System Defined Header Analysis'
942	'Message subject rewritten by Anti-Spam System Defined Header Analysis'
943	'Message quarantined by Anti-Spam System Defined Header Analysis'
944	'Message logged by Anti-Spam System Defined Header Analysis'
945	'New header added by Anti-Spam System Defined Header Analysis'
946	'Message copied by Anti-Spam System Defined Header Analysis'
947	'Message forwarded by Anti-Spam System Defined Header Analysis'
951	'Message dropped by Anti-Spam End User Spam Report'
952	'Message dropped by Anti-Spam Enterprise Spam Trap Report'
953	'Message forwarded to the global user report agent'
954	'Message repackaged to the global enterprise report agent'
961	'Message dropped by Anti-Spam Enterprise Spam Profiler'
962	'Message subject rewritten by Anti-Spam Aggregate Spam Confidence'
963	'Message quarantined by Anti-Spam Enterprise Spam Profiler'
964	'Message logged by Anti-Spam Enterprise Spam Profiler'
965	'New header added by Anti-Spam Enterprise Spam Profiler'
966	'Message copied by Anti-Spam Enterprise Spam Profiler'
967	'Message forwarded by Anti-Spam Enterprise Spam Profiler'
971	'Message dropped by Anti-Spam User Defined Header Analysis'
972	'Message subject rewritten by Anti-Spam User Defined Header Analysis'

973	'Message quarantined by Anti-Spam User Defined Header Analysis'
974	'Message logged by Anti-Spam User Defined Header Analysis'
975	'New header added by Anti-Spam User Defined Header Analysis'
976	'Message copied by Anti-Spam User Defined Header Analysis'
977	'Message forwarded by Anti-Spam User Defined Header Analysis'
978	'Secure delivery triggered by Anti Spam User Defined Header Analysis'
980	'Message detected for forged domain based on routing list.'
981	'Header added for ESP.'
Actions from within the Quarantine Queue	
1001	'Message dropped by the Queue Manager UI from SMTPO.'
1002	'Message dropped by the Queue Manager UI from Queues.'
1003	'Messages forwarded by the Queue Manager UI from the Quarantine Queue'
1004	'Messages moved by the Queue Manager UI from the Quarantine Queue'
Undeliverable Message Actions	
1101	'Undeliverable message deleted.'
1102	'Undeliverable message quarantined.'
MIME Rebuild Actions	
1201	'MIME Rebuild failed. Message dropped by Join Queue'
1202	'MIME Rebuild failed. Message quarantined by Join Queue'
1203	'MIME Rebuild failed. Original message delivered by Join Queue'
Content Extraction Actions	

2101	'Extraction failed. Message quarantined'
Failed Operations Actions	
3101	'Failure in single thread mode. Message possibly using high resources. Message quarantined'

IronMail Logs

Log Levels

IronMail allows the Administrator to configure the type of log entries that will be generated and the amount of detail that will be maintained in log files. The possible log levels are shown in the table below.

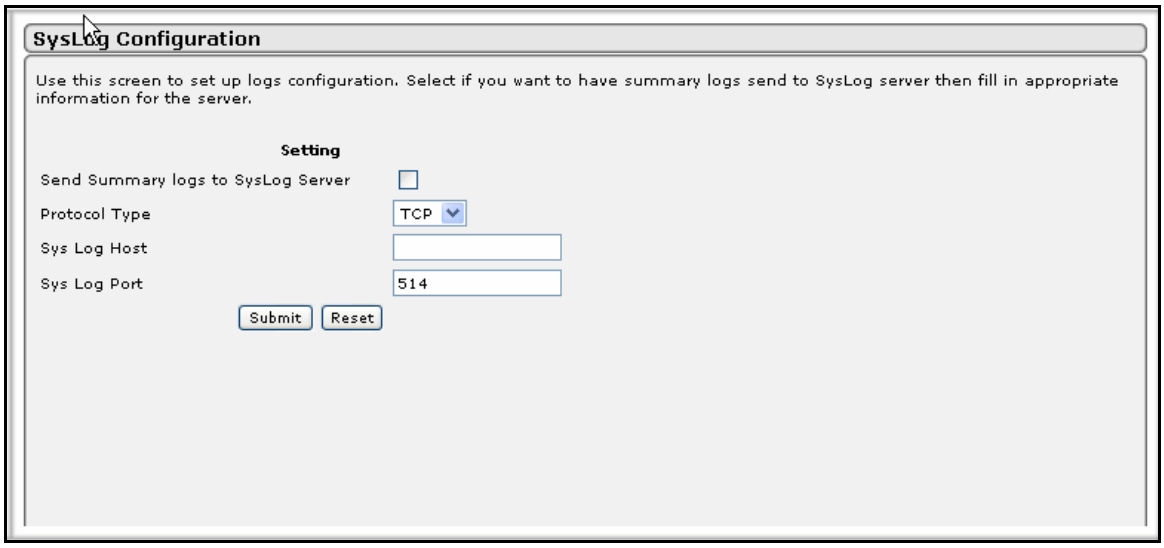
Log Level	Description
Critical	Captures information about an urgent condition, such as a general database failure.
Error	Captures information only about errors that occur that may require Administrative support or assistance from CipherTrust Support. This is the default setting when IronMail is first installed.
Information	Captures general process flow information, such as the order of functions through which messages flow, etc.
Detailed	Most verbose setting. Captures process flow in great detail, including information at the program level. Especially useful for analyzing problems, etc.

SysLog Configuration

IronMail can generate and transmit the same data it generates for its Summary Log (*Administration > Reports/Log Files >* Summary Logs) in SysLog format for integration with a network's SysLog logging system.

In addition to configuring IronMail to communicate with the SysLog server—as provided below—the SysLog server must be configured to recognize IronMail's data. IronMail uses the SysLog **User** facility and **Info** level for the data it sends. Therefore, a "user.info" variable must be created for /var/log/*ironmailname_syslog* on the receiving host.

Note: If Syslog is turned on, no information will be available on the IronMail in the Summary log.


SysLog Configuration
Use this screen to set up logs configuration. Select if you want to have summary logs send to SysLog server then fill in appropriate information for the server.
Setting
Send Summary logs to SysLog Server
Protocol Type
TCP
Sys Log Host
Sys Log Port
514
Submit
Reset

Configure IronMail's SysLog output using the four user input fields on this page:

Send Summary Logs to SysLog Server	Select the **Send Summary Logs to SysLog Server** check box to enable IronMail's SysLog output.
***Protocol* Type**	Select the *network* protocol used by the SysLog Server: TCP or UDP. (Ordinarily, SysLog uses UDP.)
SysLog Host	Enter the *IP address* or *host name* of the SysLog Server. Note that a *SysLog Server configuration* determines whether an IP address or host name should be used here. (Refer to the SysLog Server documentation.) If the Server is configured for *IP address* and its *host name* is entered here, IronMail may not be able to deliver its data to it.
SysLog Port	Enter the port number IronMail should use to connect to the SysLog Server.

Click **Submit** to save user input.

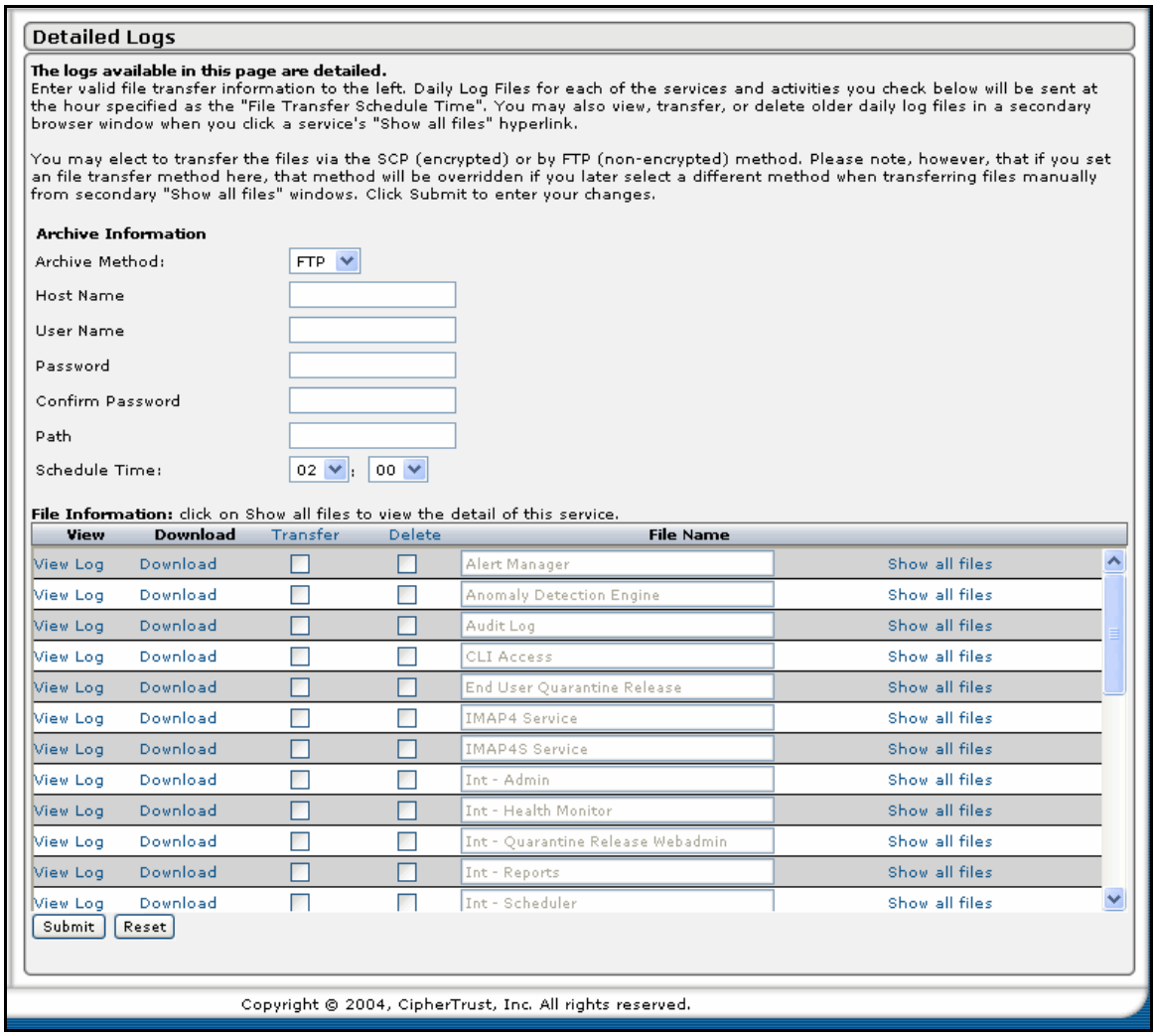
Detailed Logs

IronMail records in its Detailed Logs all the actions it takes as it processes messages. The amount of detail recorded in these logs is controlled by the Logging Level configured for each of IronMail's Queue Services and Mail Services. (For example navigate to *Mail-Firewall > Configure Mail Services > SMTPI Service > "Log Level"* in the secondary properties window for the SMTPI Service.)

Ordinarily, a log level of "Information" is adequate for day-to-day monitoring and will provide enough information to indicate that a Service is running properly, and at that level, will not bloat in size to an unmanageable level. It is recommended, however, that the logging level for Mail services (e.g., SMTPI/SMTPIS, *POP3*, POP3S, etc.) be set to "Detailed" for the first several weeks after IronMail is placed in the "mail flow" of the *network*. This will ensure that adequate information is available if troubleshooting mail-flow problems is required. Once IronMail is processing messages without incident, the logging level should be changed.

Similarly, the logging level for the Queue services (e.g., Content Filtering Queue, Anti-Spam Queue, etc.) should be raised to "Detailed" during the period that "policy testing" is underway. That level will be required to see the specific reasons a message was detected and acted upon by one of IronMail's spam or email policies. Once the *policy* testing is complete, these log levels may be changed.

In high mail-volume environments, some logs may grow very large, up to 100-200 MB in size. Log files larger than just 1 MB will typically take longer to open in IronMail's web interface than administrators will care to wait. Administrators are encouraged, then, to use an SSH client (such as the freely available "Putty" client) to open these logs. Within the command line interface, logs open instantly, and queries within them are as fast.


Detailed Logs
The logs available in this page are detailed.
Enter valid file transfer information to the left. Daily Log Files for each of the services and activities you check below will be sent at the hour specified as the "File Transfer Schedule Time". You may also view, transfer, or delete older daily log files in a secondary browser window when you click a service's "Show all files" hyperlink.
You may elect to transfer the files via the SCP (encrypted) or by FTP (non-encrypted) method. Please note, however, that if you set an file transfer method here, that method will be overridden if you later select a different method when transferring files manually from secondary "Show all files" windows. Click Submit to enter your changes.
Archive Information
Archive Method: FTP
Host Name
User Name
Password
Confirm Password
Path
Schedule Time: 02 : 00
File Information: click on Show all files to view the detail of this service.
View Download Transfer Delete File Name
View Log Download Alert Manager Show all files
View Log Download Anomaly Detection Engine Show all files
View Log Download Audit Log Show all files
View Log Download CLI Access Show all files
View Log Download End User Quarantine Release Show all files
View Log Download IMAP4 Service Show all files
View Log Download IMAP4S Service Show all files
View Log Download Int - Admin Show all files
View Log Download Int - Health Monitor Show all files
View Log Download Int - Quarantine Release Webadmin Show all files
View Log Download Int - Reports Show all files
View Log Download Int - Scheduler Show all files
Submit Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

IronMail generates Detailed Logs, covering all aspects of its core functionality:

- **WebAdmin:** The WebAdmin log reports every action or command that occurs within the Web Admin interface. For example, if users view or download a log, that action will be reported in this log.
- **Admin:** The Admin log reports every connection to IronMail via the command line interface, and all commands invoked during that administration session.
- **Alert Manager:** This log records all of the information about the alerts that IronMail generates.
- **Health Monitor:** The Health Monitor reports every system test it performs, and their results.
- **Audit Log:** The Audit Log reports the timestamp, user, and page name each time a page in IronMail's graphical user interface is accessed.

- **SMTPI Service:** SMTPI is IronMail's service that processes all email coming into the appliance via a non-secure port. This log reports the details of when it "wakes up" to process new incoming messages, and what it does with them.
- **SMTPIS Service:** SMTPIS is IronMail's service that processes all email coming into the appliance via a secure port. This log reports the details of when it "wakes up" to process new incoming messages, and what it does with them.
- **SMTPO Service:** SMTPO is IronMail's service that processes all email delivered out of the appliance. This log reports the details of when it "wakes up" to process outgoing messages, and what it does with them.
- **POP3 Service:** The POP3 Service processes message retrieval via the POP3 *protocol*. This log reports the details of when it responds to a user's POP request.
- **POP3S Service:** The POP3S Service processes message retrieval via the POP3S protocol. This log reports the details of when it responds to a user's secure POP request.
- ***IMAP4* Service:** The IMAP4 Service processes message retrieval via the IMAP4 protocol. This log reports the details of when it responds to a user's IMAP request.
- **IMAP4S Service:** The IMAP4 Service processes message retrieval via the IMAP4 protocol. This log reports the details of when it responds to a user's secure IMAP request.
- **IronWebMail:** IronWebMail proxies HTTP and HTTPS webmail. This log reports all its activity as it sends and retrieves mail using these protocols.
- **Scheduler LDAPSync:** If LDAP is configured on the appliance, the LDAP Sync service "communicates" with the LDAP server on a regular basis. This log reports the details of its activity.
- **Scheduler:** This log details scheduled activities such as file transfers, etc.
- **SSH:** This log details activities conducted through the secure shell (command line).
- **Anomaly Detection Engine:** If IronMail's Anomaly Detection Engine is configured on the appliance, this log will record all of its activity.
- **Queue - Virus Scan:** The Virus Scan log reports the details of its activity each time it "wakes up" to check messages for viruses.
- **Queue - Content Filtering:** The Content Filtering Queue log reports the details of its activity each time it "wakes up" to apply the Attachment Filtering, Message Stamping, and Content Filtering policies to email.
- **Queue - Mail Monitoring:** The Mail Monitoring Queue log reports the details of its activity each time it "wakes up" to apply the Off-Hour Delivery, Mail Monitoring, and Encrypted Message Filtering policies to email.
- **Internal Queue - *MIME* Ripper:** The MIME Ripper is an internal queue, and the first to process messages. This log reports the details of its activities when it "wakes up" to break every incoming message into its separate parts.
- **Internal Queue - MIME Joiner:** The MIME Joiner is an internal queue, and the last to process messages before the SMTPO service finally delivers them out of the appliance. This log reports the details of its activities when it "wakes up" to join the message's parts back into a whole.
- **Internal Queue - Quarantine:** The Quarantine Queue log reports the details of its activity each time it "wakes up" to process messages that other queues have sent to it.

- **Queue - Anti-Spam:** The Anti-Spam Queue log reports the details of its activity each time it "wakes up" to apply IronMail's anti-spam policies to email.
- **Secure Web Delivery:** This log will record all of IronMail's action related to Secure Web Delivery.
- **Cleanup:** The Cleanup log reports the details of its activity each time the IronMail scheduler runs.
- **End User Quarantine Release:** There are two logs pertaining to the End User Quarantine Release process that report the detailed of quarantine release activity: eusrquarantine.log and ct_euser.log. These logs, which are viewable in the Command Line Interface, are useful for creating whitelist entries based on the messages releases by end users.
- **Reports Log:** The Reports log reports the details of its activity each time IronMail runs reports.
- **FTP Log:** This log reports the details of its activity each time IronMail runs FTP processes.

Note: IronMail generates one other detailed log, **IronMail Setup.** Generated only once, after the initial IronMail setup and configuration, this log reports the details of the setup process.

IronMail can transfer Detailed Log files to an archive server, either manually or automatically. If archive server information is provided in the **Archive Information** input fields at the top of the page and the **Transfer** check box is selected in the table below, IronMail will automatically transfer the files at the specified hour. When the **Archive Information** input fields are left blank, or if the **Transfer** check box is de-selected in the table below, Detailed Logs may be manually transferred by entering archive server information in the secondary browser window that opens when clicking the **Show all files** hyperlink.

The automatic transfer of Detailed Log files requires the following user input:

Archive Method	Select an archive method IronMail should use when transferring the log files: • **SCP:** Select SCP to transfer the files securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the files in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command.
Host Name	Enter the host name of the archive server.
Username	Enter a valid username with SCP or FTP privileges.
Password	Enter and confirm a valid password.
Path	Enter the path string to the location on the archive server where IronMail should transfer the files. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the files.

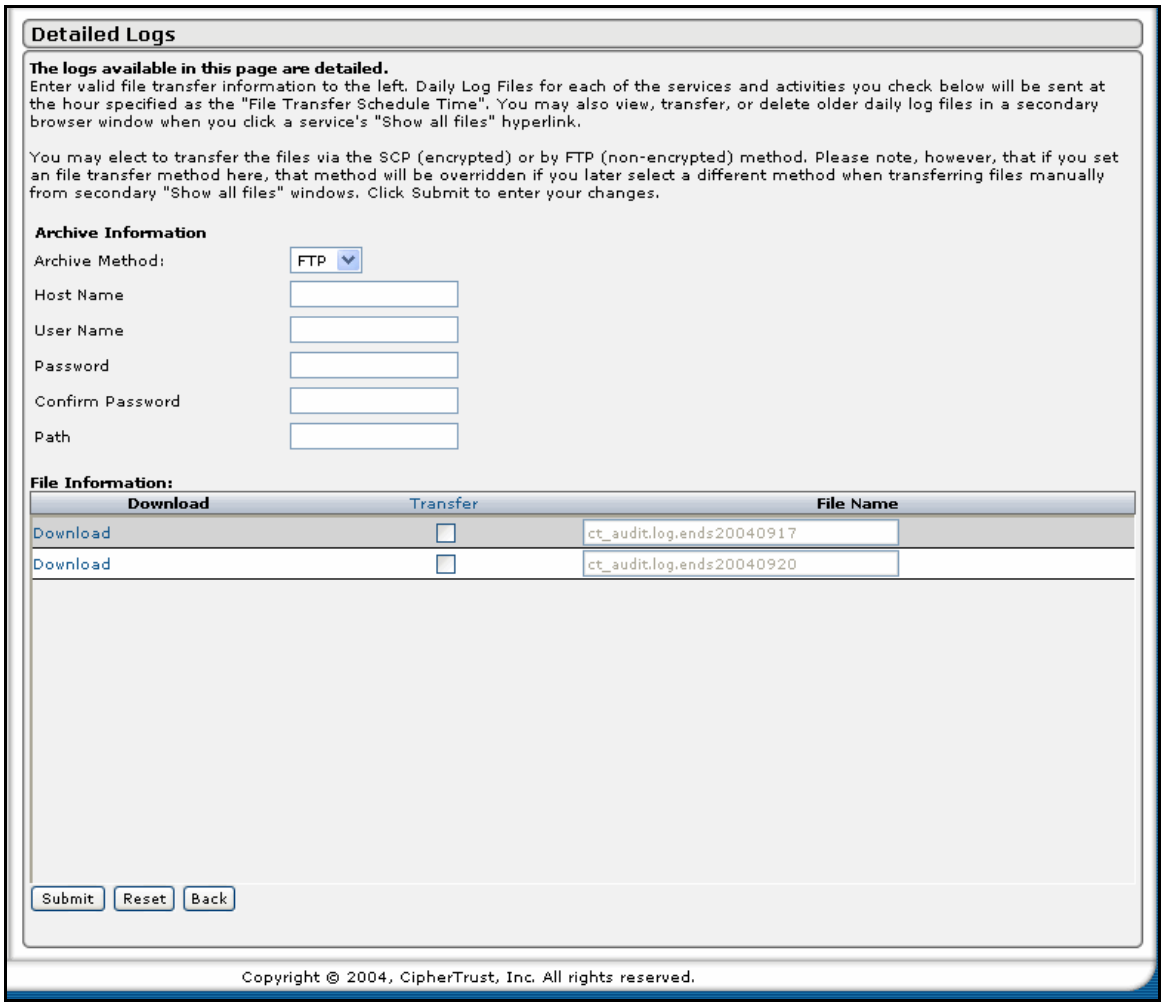
To configure IronMail for manual Detailed Log file delivery only, do not enter file transfer information on this page. For manual file transfer, enter the file transfer information in the secondary browser window that opens when clicking the **Show all files** hyperlink in the table of files below.

Below the **Archive Information** input fields is a table listing the names of all available log files. The logs within this window are current for today—all IronMail processes that have occurred since midnight, up to the moment a **View** or **Download** action is taken.

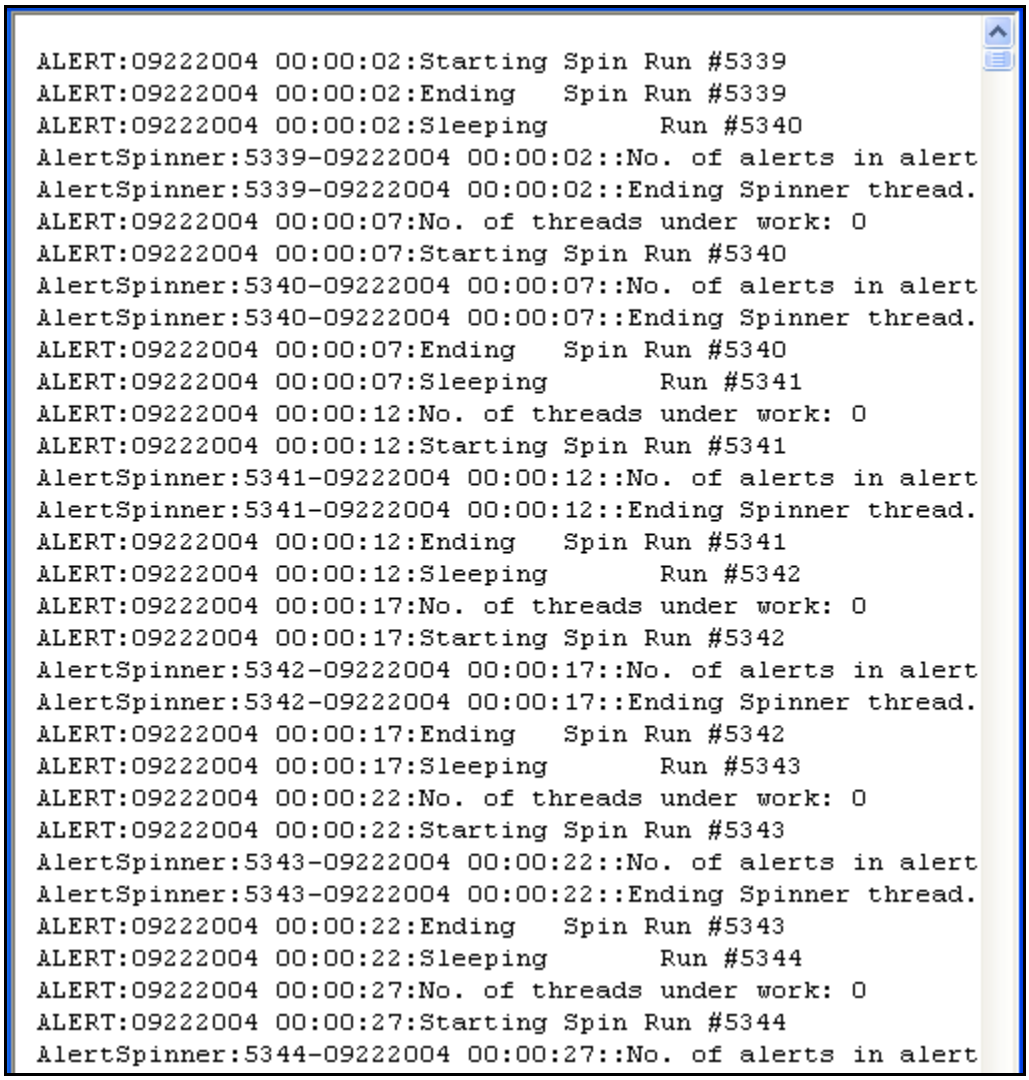
The table of Detailed Logs offers the following information and actions:

View	The "magnifying glass" icon in this column is a hyperlink that opens the contents of today's Detailed Log file in a secondary browser window. Note that in high mail-volume environments (50,000+ per day), this file may be extremely large and in some environments has taken up to 4 hours to load in a browser.
Download	The "magnifying glass" icon in this column is a hyperlink that opens a "Save As..." dialog allowing the administrator to save the file to disk.
Transfer	If the **Transfer** check box is selected and Archive Information is provided in the input fields above, IronMail will automatically transfer any selected Detailed Log file at the scheduled hour. Click **Submit** after selecting a **Transfer** check box to save the user input.
Delete	If the **Delete** check box is selected, click **Submit** to delete the most recent (yesterday's) Detailed Log file.
File Name	This column identifies the name of each log. (Note that because IronMail archives these files at approximately 3:30 AM, each day's Detailed Log files are not available for file transfer until the next morning.
Show all files	The **Show all files** hyperlink opens a secondary browser window that displays all Detailed Log files that IronMail's Cleanup Schedule has not yet deleted from disk. (Note that each file name includes the date that the file was generated—a date one day older than then data contained within it. The file for "20030121" was generated on January 21, 2003, but contains the raw data for messages processed by IronMail on January 20, 2003.)

When the **Show all files** hyperlink is clicked, a window opens, displaying any Detailed Logs that have not yet been deleted by IronMail's Cleanup Schedule. Enter Archive Information in the six input fields at the top of the window, and select the **Download** links or the**Transfer** check boxes for specific files.


Detailed Logs
The logs available in this page are detailed.
Enter valid file transfer information to the left. Daily Log Files for each of the services and activities you check below will be sent at the hour specified as the "File Transfer Schedule Time". You may also view, transfer, or delete older daily log files in a secondary browser window when you click a service's "Show all files" hyperlink.
You may elect to transfer the files via the SCP (encrypted) or by FTP (non-encrypted) method. Please note, however, that if you set an file transfer method here, that method will be overridden if you later select a different method when transferring files manually from secondary "Show all files" windows. Click Submit to enter your changes.
Archive Information
Archive Method:
FTP
Host Name
User Name
Password
Confirm Password
Path
File Information:
Download
Transfer
File Name
Download
ct_audit.log.ends20040917
Download
ct_audit.log.ends20040920
Submit
Reset
Back
Copyright © 2004, CipherTrust, Inc. All rights reserved.

An example of a detailed log (for the Alert service) is shown below.



```
ALERT:09222004 00:00:02:Starting Spin Run #5339
ALERT:09222004 00:00:02:Ending   Spin Run #5339
ALERT:09222004 00:00:02:Sleeping       Run #5340
AlertSpinner:5339-09222004 00:00:02::No. of alerts in alert
AlertSpinner:5339-09222004 00:00:02::Ending Spinner thread.
ALERT:09222004 00:00:07:No. of threads under work: 0
ALERT:09222004 00:00:07:Starting Spin Run #5340
AlertSpinner:5340-09222004 00:00:07::No. of alerts in alert
AlertSpinner:5340-09222004 00:00:07::Ending Spinner thread.
ALERT:09222004 00:00:07:Ending   Spin Run #5340
ALERT:09222004 00:00:07:Sleeping       Run #5341
ALERT:09222004 00:00:12:No. of threads under work: 0
ALERT:09222004 00:00:12:Starting Spin Run #5341
AlertSpinner:5341-09222004 00:00:12::No. of alerts in alert
AlertSpinner:5341-09222004 00:00:12::Ending Spinner thread.
ALERT:09222004 00:00:12:Ending   Spin Run #5341
ALERT:09222004 00:00:12:Sleeping       Run #5342
ALERT:09222004 00:00:17:No. of threads under work: 0
ALERT:09222004 00:00:17:Starting Spin Run #5342
AlertSpinner:5342-09222004 00:00:17::No. of alerts in alert
AlertSpinner:5342-09222004 00:00:17::Ending Spinner thread.
ALERT:09222004 00:00:17:Ending   Spin Run #5342
ALERT:09222004 00:00:17:Sleeping       Run #5343
ALERT:09222004 00:00:22:No. of threads under work: 0
ALERT:09222004 00:00:22:Starting Spin Run #5343
AlertSpinner:5343-09222004 00:00:22::No. of alerts in alert
AlertSpinner:5343-09222004 00:00:22::Ending Spinner thread.
ALERT:09222004 00:00:22:Ending   Spin Run #5343
ALERT:09222004 00:00:22:Sleeping       Run #5344
ALERT:09222004 00:00:27:No. of threads under work: 0
ALERT:09222004 00:00:27:Starting Spin Run #5344
AlertSpinner:5344-09222004 00:00:27::No. of alerts in alert
```

Understanding Detailed Logs

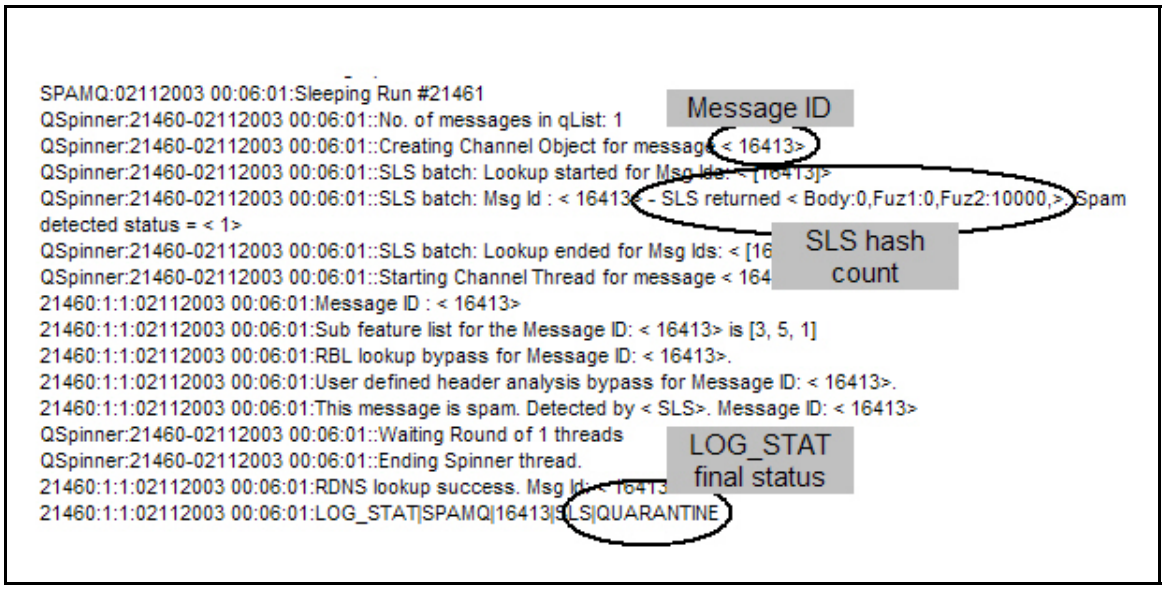
IronMail's Detailed Logs report very detailed information—if the Mail or Queue Service's logging level was set high enough—about how each service or subsystem processes a message. IronMail was designed to write to these logs in real time as it performs each step of its message-processing. The "output," however, can be somewhat cryptic—even bewildering—to first-time log readers. View the following pages to learn how to read these log files: Anti-Spam Queue Detailed Log (spamq), Content Filtering Detailed Log (cfq), and SMTPI Service Detailed Log (smtpproxy).

Anti-Spam Queue Detailed Log

The SpamQ log is very similar to the CFQ log, except a message's Message ID must first be obtained from the SMTPPROXY log before it can be found within it or accessed using the Queue Manger.

Note: As a convenience you can obtain the Message ID by selecting *Queue Manage r> Queue Information* to display a list of Queues. Click on the Anti-Spam Queue Name in the Queue Information screen and locate the ID on the Message Header window. You can also search for locate the message ID using the results from a Quarantined Message or Processed Message search.

To get the Message ID from the SMTPPROXY log see the following illustration. Specific message information is displayed on lines beginning with a spin, channel and thread number.


SPAMQ:02112003 00:06:01:Sleeping Run #21461
QSpinner:21460-02112003 00:06:01::No. of messages in qList: 1
Message ID
QSpinner:21460-02112003 00:06:01::Creating Channel Object for message < 16413>
QSpinner:21460-02112003 00:06:01::SLS batch: Lookup started for Msg Ids: < [16413]>
QSpinner:21460-02112003 00:06:01::SLS batch: Msg Id : < 16413> - SLS returned < Body:0,Fuz1:0,Fuz2:10000,> Spam detected status = < 1>
SLS hash count
QSpinner:21460-02112003 00:06:01::SLS batch: Lookup ended for Msg Ids: < [16
QSpinner:21460-02112003 00:06:01::Starting Channel Thread for message < 164
21460:1:1:02112003 00:06:01:Message ID : < 16413>
21460:1:1:02112003 00:06:01:Sub feature list for the Message ID: < 16413> is [3, 5, 1]
21460:1:1:02112003 00:06:01:RBL lookup bypass for Message ID: < 16413>.
21460:1:1:02112003 00:06:01:User defined header analysis bypass for Message ID: < 16413>.
21460:1:1:02112003 00:06:01:This message is spam. Detected by < SLS>. Message ID: < 16413>
QSpinner:21460-02112003 00:06:01::Waiting Round of 1 threads
QSpinner:21460-02112003 00:06:01::Ending Spinner thread.
LOG_STAT final status
21460:1:1:02112003 00:06:01:RDNS lookup success. Msg Id: < 16413
21460:1:1:02112003 00:06:01:LOG_STAT|SPAMQ|16413|SLS|QUARANTINE

Administrators typically perform a query for a specific message ID. They note the channel and thread number associated with that message ID, and "follow the trail of bread crumbs"—i.e. the channel and thread number—to the "LOG_STAT" entries. Between the first and last channel and thread lines, IronMail reports each of the anti-spam tools that examined the message, and the results of their examination. The actual spam-blocking processes are identified immediately following the timestamp: SLS (Statistical Lookup Service), RBL (Realtime Blackhole List), RDNS (reverse DNS), MF (System Defined Header Analysis), etc., and the values they returned.

Content Filtering Queue Detailed Log

IronMail is capable of processing many messages in the Content Filtering Queue at the same time. Because of this, lines providing information about one particular message may be commingled with lines providing information about other messages. (The Content Filtering Queue log file does not group the lines in the log by message.) Whereas administrators use a message's *IP address* as the "trail of bread crumbs" in the SMTPPROXY log, they must use the message's channel and thread number to track a message here in the Content Filtering Queue (CFQ) log.

Lines in the log file that begin with "CFQ" indicate that the Content Filtering Queue is beginning and ending "spins"—that is, an internal process to examine a set of messages. Lines that begin with "QSpinner" provide information about the "spin." Lines that begin with a numeric string provide information about specific messages.

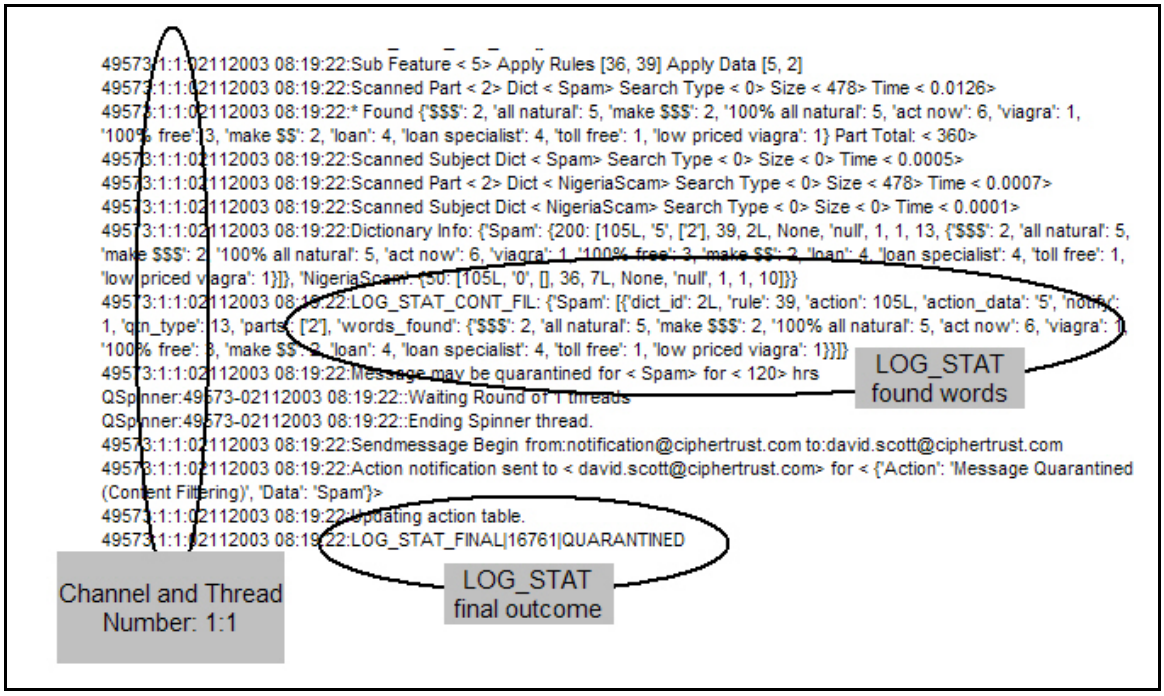
```
CFQ:02112003 00:00:17:No. of threads under work: 0
CFQ:02112003 00:00:17:Starting Spin Run #46585
CFQ:02112003 00:00:17:Ending Spin Run #46585
CFQ:02112003 00:00:17:Sleeping Run #46586
QSpinner:46585-02112003 00:00:17::No. of messages in qList: 0
QSpinner:46585-02112003 00:00:17::Ending Spinner thread.
```

For lines in the CFQ log that begin with numbers, the first set identifies the spin that IronMail creates to process a batch of messages. (Several times a minute, on a dynamic schedule depending on current message load, IronMail generates a new spin to process the next batch of newly available messages.) The spin number terminates with a colon. The number immediately following the spin number is the channel IronMail creates within the spin. (IronMail will create multiple channels, if necessary, to process a large number of messages within a single spin.) A

colon terminates the channel number. Following the channel number is the thread—a number associated with each email processed within that channel.

```
46602:1:1:02112003 00:03:08:Part < 1> Type < > Xtn < txt> Format < 2>
46602:1:1:02112003 00:03:08:Sub Feature < 4> Apply Rules [] Apply Data []
46602:1:1:02112003 00:03:08:Looking for xtns - {1: {}, 0: {}}
46602:1:1:02112003 00:03:08:LOG_STAT_ATT_FIL: {}
46602:1:1:02112003 00:03:08:Sub Feature < 5> Apply Rules [36, 12, 39] Apply Data [5, 4, 2]
46602:1:1:02112003 00:03:08:Scanned Subject Dict < Porn> Search Type < 0> Size < 16> Time < 0.0028>
46602:1:1:02112003 00:03:08:Scanned Part < 1> Dict < Porn> Search Type < 0> Size < 648> Time < 0.0221>
46602:1:1:02112003 00:03:08:Scanned Subject Dict < NigeriaScam> Search Type < 0> Size < 16> Time < 0.0002>
46602:1:1:02112003 00:03:08:Scanned Part < 1> Dict < NigeriaScam> Search Type < 0> Size < 648> Time < 0.0009>
46602:1:1:02112003 00:03:08:Scanned Subject Dict < Spam> Search Type < 0> Size < 16> Time < 0.0022>
46602:1:1:02112003 00:03:08:Scanned Part < 1> Dict < Spam> Search Type < 0> Size < 648> Time < 0.0155>
46602:1:1:02112003 00:03:08:Dictionary Info: {'Porn': {50: [105L, '5', [], 12, 4L, None, 'null', 1, 1, 9]}, 'NigeriaScam': {50: [105L,
'0', [], 36, 7L, None, 'null', 1, 1, 10]}, 'Spam': {200: [105L, '5', [], 39, 2L, None, 'null', 1, 1, 13]}}
46602:1:1:02112003 00:03:08:LOG_STAT_CONT_FIL: {}
46602:1:1:02112003 00:03:08:LOG_STAT_FINAL|16404|PUSHED TO NEXT Q
46602:1:1:02112003 00:03:08:Channel thread Ended for message < 16404>
```

The Content Filtering Queue processes Attachment Filtering, Message Stamping, and Content Filtering policies. The CFQ log, therefore, will show each *policy* being enforced, and the resulting action, if applicable. The text string "LOG_STAT_" will identify the conclusion of each enforced policy, and appended to the "LOG_STAT_" string will be an abbreviated name of the specific policy that was enforced. (For example, "LOG_STAT_ATT_FIL" is shorthand for "Finished processing the Attachment Filtering policies," and "LOG_STAT_CONT_FIL" is shorthand for "Finished processing the Content Filtering policies.")



A typical reason for using the Detailed CFQ log is to find which dictionary words IronMail detected causing it to conclude that a message was spam or pornography. Administrators will search for the From: email address of the message in question. The query will return the first instance of the From: address in the log file. However, because the user may have sent many messages that day, the administrator uses the message's timestamp to identify the one he or she is looking for.

He or she will repeat the search until the reported timestamp is from 15-45 seconds *after* the SMTPI Service's timestamp. (Depending on message load and the order of the Content Filtering Queue, it may take some number of seconds for a message to be picked up by the CFQ after the SMTPI Service processes it.) Administrators verify that the From: and To: addresses reported in the CFQ log match the message for which they are looking. Then they note the spin, channel, and thread number for that message. They scroll through the log, following the channel and thread number until they arrive at the "LOG_STAT line" for the policy that acted upon the message. A "LOG_STAT_" followed by empty curly braces ("{ }") means that nothing in the message met the condition of the policy. If the curly braces contain any text whatsoever, then conditions of a policy were detected and the policy's action was taken. Scroll upwards from the "LOG_STAT_" entry and read details about what IronMail detected.

Note that IronMail performs its policy enforcement on all parts of a message (if the policy was so configured), and the log will report for as many parts as exist in the message, that the policy was being enforced. In every instance, when IronMail detects any part of the message that met a condition of the policy, the values are reported.

SMTPProxy Detailed Log

IronMail's SMTPI Service, responsible for processing messages when they first arrive at the IronMail, generates the SMTPPROXY Log, one of the more important Detailed Log files to use. Administrators will typically use this log to:

- Verify that IronMail even received a message. (If IronMail received the message, then troubleshooting message delivery issues will be different than if IronMail never received the message in the first place.)
- Acquire a message's unique Message ID number. (Many of the detailed log files reference a message by its Message ID. To find a particular message in IronMail's Spam Queue log, for example, the administrator must first extract the message's unique Message ID number from the SMTPPROXY Log.)

There is an order to how data is displayed in the SMTPPROXY log. For example, administrators will observe that a certain group of lines beginning with the string "SMTPPROXY" will always display together and repeat throughout the log. The text string "SMTPPROXY" at the beginning of these lines is always immediately followed by a date and timestamp (01212003 10:14:05). The text that immediately follows the date and timestamp on these lines indicates that IronMail's SMTPI Service is "waking up" to process a batch of messages, and depending on how many messages are ready to be processed, setting load throttling values. Throughout the log, IronMail's SMTPI Service is seen "waking up" to process new messages. These "SMTPPROXY lines" always mark the beginning of a new round of processing.

```
SMTPPROXY:02112003 00:03:34:Governor - Starting Spin Run #1511
SMTPPROXY:02112003 00:03:34:No. of threads under work: 0
SMTPPROXY:02112003 00:03:34:Message Percentage - < 0>
SMTPPROXY:02112003 00:03:34:Matrix Index - < 0> Message Matrix - < 1> Thread Matrix - < 100>
SMTPPROXY:02112003 00:03:34:Setting threshold level to - < 100>
SMTPPROXY:02112003 00:03:34:Governor - Ending Spin Run #1511
```

Administrators will also observe that there are large blocks of the log where each line begins with an *IP address*. These blocks of "IP address lines" pertain to all the individual messages that the SMTPI Service processes during a current "cycle." The IP address of each message the SMTPI Service picked up to process is presented.

```
172.16.0.7-2698:02112003 00:04:13:Relay ----> < 1>
172.16.0.7-2698:02112003 00:04:13:Skipping all queues since connection is from IronMail itself
65.125.145.129-63771:02112003 00:04:19:Relay ----> < 0>
65.125.145.129-63771:02112003 00:04:19:Parsed Data < petelind@spiresecurity.com> addr, < petelind> UID , < spirese
65.125.145.129-63771:02112003 00:04:19:Parsed Data < manthony@ciphertrust.com> addr, < manthony> UID , < ciphe
65.125.145.129-63771:02112003 00:04:19:QUEU COMMAND RECEIVED (' < petelind@spiresecurity.com> size=2077', 'p
['manthony@ciphertrust.com'], 'inout': [], 'out': []}, {'in': [' < manthony@ciphertrust.com>'], 'inout': [], 'out': []}, '65.125.145.1
65.125.145.129-63771:02112003 00:04:19:Close Data File /ct/data/mss/00/00/00/16/412
65.125.145.129-63771:02112003 00:04:19:Created new Message ID - 16412 File - /ct/data/mss/00/00/00/16/412
65.125.145.129-63771:02112003 00:04:19:LOG_STAT|petelind@spiresecurity.com|[\'manthony@ciphertrust.com\']|2940
65.125.145.129-63771:02112003 00:04:19:('65.125.145.129', 63771)- -Mail dispatch time > 0.148196935654
68.81.95.196-3404:02112003 00:05:05:Relay ----> < 0>
68.81.95.196-3404:02112003 00:05:11:Parsed Data < work5789xpfo@cs.com> addr, < work5789xpfo> UID , < cs.com
68.81.95.196-3404:02112003 00:05:19:Parsed Data < sam.garcia@ciphertrust.com> addr, < sam.garcia> UID , < ciphert
68.81.95.196-3404:02112003 00:05:22:QUEU COMMAND RECEIVED (' < work5789xpfo@cs.com>', 'work5789xpfo@cs
[]}, {'in': [' < sam.garcia@ciphertrust.com>'], 'inout': [], 'out': []}, '68.81.95.196', 0, 0, 5, 'cs.com')
```

When the last message has been processed in that particular "cycle," the SMTPI Service will "sleep" again until the next time it must "wake up" to process newly arrived messages. Over and over, the SMTPPROXY log repeats the same process.

The first line in a block of "IP address lines" begins with the IP address of the first message IronMail processes in that cycle. This is the IP address of a message sender—the source IP. The IP address is immediately followed by the date and timestamp when the SMTPI Service accepted the message for processing. Following the timestamp is "Relay ----> <0>" (or "Relay --> <1>"). A "0" indicates that the IP address does not appear in IronMail's Allow Relay List. (A "1" indicates that the address is on the Allow Relay List.)

```
172.16.0.7-2698:02112003 00:04:13:Relay ----> < 1>
```

Because IronMail can process multiple messages simultaneously, other messages received at the same time may be interspersed within this log. That is, their IP addresses will appear immediately above or below the IP addresses of other messages. (The SMTPPROXY log does not group its information by IP address.) The key to tracking the SMTPI Service's actions on a message is to "follow the IP address" like a trail of bread crumbs.

Following the IP address is the date and timestamp when IronMail received the message. In the text that follows, the message's From address, To address, and other information is reported.

```
65.125.145.129-63771:02112003 00:04:19:Parsed Data < petelind@spiresecurity.com> addr, < petelind> UID , < spiresecurity.com> mdomain
```

IronMail provides a visual clue in all its logs to let administrators know when it has finished doing something important: the text string "LOG_STAT_" (followed by descriptive text) is displayed in all uppercase letters. (***Note that IronMail only supplies the LOG_STAT" string for messages addressed to users in internal domains it hosts.*** Similarly, the SMTPO Detailed Log only provides the LOG_STAT string for messages addressed to users in external domains.) In the SMTPPROXY log, "LOG_STAT" indicates that the SMTPI Service has finished processing the message and is ready to send it to the next queue for additional processing. The line immediately preceding "LOG_STAT" reports that the SMTPI Service "Created new Message ID – *nnn* File"—a unique number identifying the message IronMail just processed. The Message ID number is the key to finding the same message in some of IronMail's other logs.

A typical scenario for using the SMTPPROXY is when one of IronMail's anti-spam tools send a message to a quarantine queue, and the administrator wants to find out the specific thresholds or query-results that triggered the action. Because the quarantine queue identifies the timestamp when the message was received by the SMTPI Service, the administrator performs a search in the SMTPPROXY log based on the hour, minute, and second. The administrator notes the IP address at the beginning of the line where the timestamp appears, and then scrolls down the log until he or she arrives at the line containing the text string "LOG_STAT" for that IP address. Immediately above the "LOG_STAT line" is the Message ID. The administrator uses this message ID number to find that same message in the Spam Queue log.

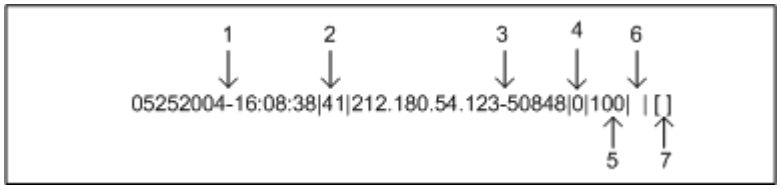
Note that the SMTPI, SMTPIS, *POP3*, POP3S, *IMAP4*, and IMAP4S detailed logs may occasionally report error messages similar to the following:

SMTPPROXY-Monitor:: Error in server select call

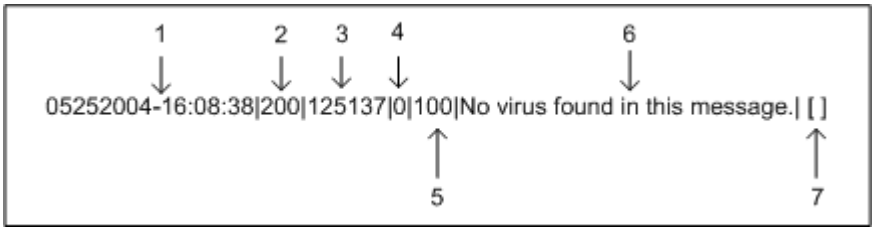
This occurs when one of IronMail's Mail Services that "listens" for email connections is stopped, either manually or because of a program error.

Summary Logs

Whereas the Detailed Log files record the specific actions IronMail takes when processing messages, the information is spread across multiple files. This Summary Log consolidates all message processing data into one file, and displays the information in a slightly different way. If IronMail does not accept a message (e.g., the sending *IP address* is on IronMail's Local Deny List and the message is dropped by the SMTPI Service), the only line in the Summary Log for that message will look like the following:



If IronMail accepted and processed the message, the first line of the Summary Log for that message will look like the following:



For messages that IronMail processed, each IronMail Queue process will write a separate line indicating what action it took on the message. To view all the lines in the Summary Log for a single message, use the "grep" command on the message ID.

The Summary Log displays seven pipe-separated ("|") fields of data. Each line in the Summary Log displays information about each IronMail process that examined or processed a message. Note that the descriptions of IronMail processes are not grouped together by message. The processes of multiple messages are commingled. As with the Detailed Logs, administrators must follow the "trail of bread crumbs" using the "Message Identifier" to trace a single message in this log. The Summary Log may be viewed in "real time" for troubleshooting and policy-tuning purposes, or it may be exported so that a third party application can perform advanced grouping, sorting, and querying within it.

The **first field** is the date and timestamp when the message was received by the SMTPI Service.

The **second field** is the "process ID"—a number used internally by IronMail to identify which IronMail processes are processing a message. For example, the JoinQ has one process number, while the SMTPO Service has another process number.

The **third field** is the "message identifier"—a number IronMail uses to uniquely identify a message. If the message is *accepted* by the SMTPI Service, the "message identifier" becomes the Message ID. See the first sample log entry above.

However, if the message is *not accepted* by IronMail (for example, the message is from an IP address that appears on a Deny List), this value will be the source IP address and port number. See the second sample log entry above.

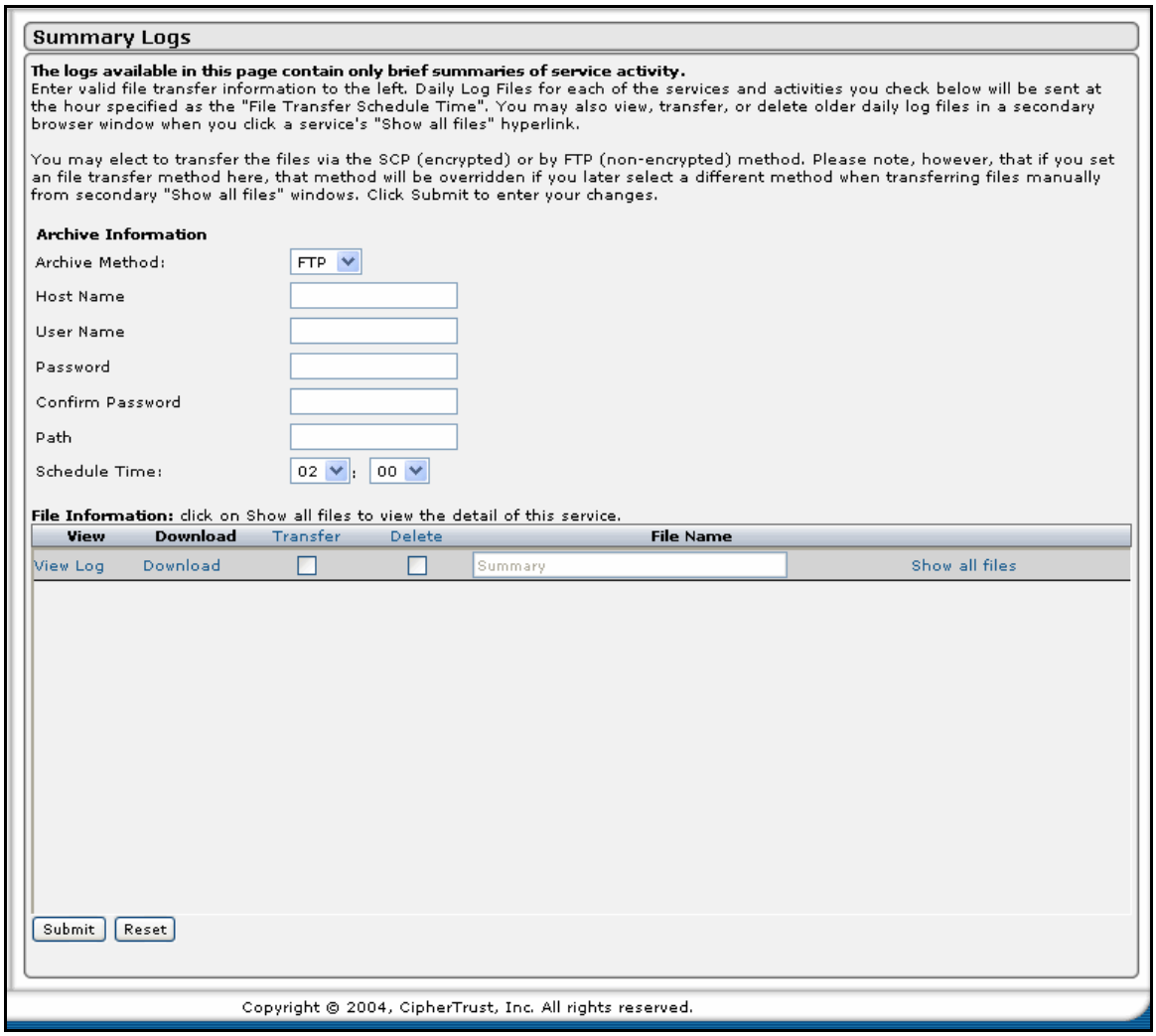
The **fourth field** is the "Action" number—a "0" or "1"—indicating whether IronMail took an action on the message because of the rules of an email *policy*. A "0" means no action was taken—the message passed straight through IronMail untouched. A "1" means that IronMail performed some action on the message.

The **fifth field** is an internal numeric code representing the action IronMail took—a number representing, for example, whether IronMail stamped an outgoing message with a footer, or deleted a file attachment, etc. (See Action Codes for a list of all IronMail actions.)

The **sixth field** displays textual information returned by the process. For example, process "21" (the SMTPI Service) will return the Mail From, Mail To, and Message ID number of a message, and the "200" process (the Virus Scan Queue) will report "No virus found in this message."

The **seventh field** displays any details about the action as applicable. For example, a Mail Monitoring *rule* based on a particular Subject will have the text of the rule's Subject displayed here.

IronMail can transfer Summary Log files to an archive server, either manually or automatically. If archive server information is provided in the six Archive Information input fields at the top of the page and the **Transfer** check box is selected in the table below, IronMail will automatically transfer the files at the specified hour. When the Archive Information input fields are left blank, or if the **Transfer** check box is de-selected in the table below, Summary Logs may be manually transferred by entering archive server information in the secondary browser window that opens when clicking the **Show all files** hyperlink.


Summary Logs
The logs available in this page contain only brief summaries of service activity.
Enter valid file transfer information to the left. Daily Log Files for each of the services and activities you check below will be sent at the hour specified as the "File Transfer Schedule Time". You may also view, transfer, or delete older daily log files in a secondary browser window when you click a service's "Show all files" hyperlink.
You may elect to transfer the files via the SCP (encrypted) or by FTP (non-encrypted) method. Please note, however, that if you set an file transfer method here, that method will be overridden if you later select a different method when transferring files manually from secondary "Show all files" windows. Click Submit to enter your changes.
Archive Information
Archive Method:
FTP
Host Name
User Name
Password
Confirm Password
Path
Schedule Time:
02
00
File Information: click on Show all files to view the detail of this service.
View
Download
Transfer
Delete
File Name
View Log
Download
Summary
Show all files
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

The automatic transfer of Summary Log files requires the following user input:

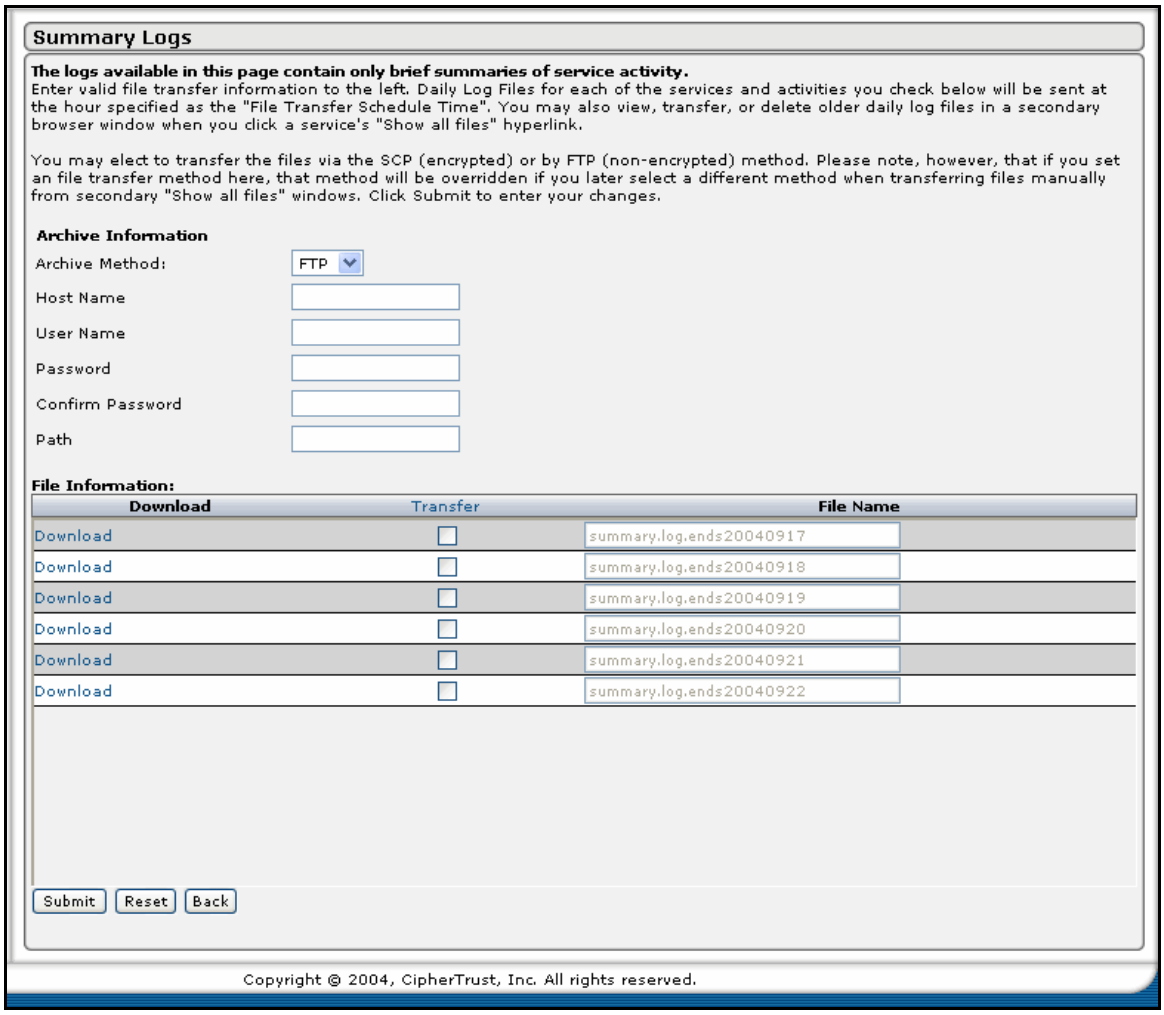
Archive Method	Select an archive method IronMail should use when transferring the Summary Log files: • **SCP:** Select SCP to transfer the files securely using the SCP *protocol*. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the files in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files to the same directory, earlier files will be over-written with later IronMail transfers.
Host Name	Enter the host name of the archive server.
Username	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.
Path	Enter the path string to the location on the archive server where IronMail should transfer the files. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are:

	"/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the files.

The lower portion of the screen displays the following options:

View Log	The View Log hyperlink opens the contents of the most recent (yesterday's) Summary Log file in a secondary window. In high mail-volume environments (50,000+ per day), this file may be extremely large and in some environments it has taken considerable time to load in a browser. Consider viewing this log within an SSH client from IronMail's command line interface.)
Download	The Download hyperlink opens a "Save As..." dialog allowing the Administrator to save the file to disk.
Transfer	If the **Transfer** check box is selected and Archive Information is provided in the input fields above, IronMail will automatically transfer the Summary Log file at the scheduled hour. Click **Submit** after selecting **Transfer** to save the user input.
Delete	If the **Delete** check box is selected, click **Submit** to delete the most recent (yesterday's) Summary Log file.
File Name	This column identifies the name of the most recent file. (Note that because IronMail generates these files at approximately 12:30 AM, each day's Summary Log data does not become available for file transfer until the next morning.
Show all files	The **Show all files** hyperlink opens a secondary browser window that displays all Summary Log files that IronMail's Cleanup Schedule has not yet deleted from disk. (Note that each file name includes the date that the file was generated—a date one day older than then data contained within it. The file for "20030121" was generated on January 21, 2003, but contains the raw data for messages processed by IronMail on January 20, 2003.)

To configure IronMail for manual Summary Log file delivery only, do not enter file transfer information on this page. For manual file transfer, enter the file transfer information in the secondary browser window that opens when clicking the **Show all files** hyperlink in the table of files below.


Summary Logs
The logs available in this page contain only brief summaries of service activity.
Enter valid file transfer information to the left. Daily Log Files for each of the services and activities you check below will be sent at the hour specified as the "File Transfer Schedule Time". You may also view, transfer, or delete older daily log files in a secondary browser window when you click a service's "Show all files" hyperlink.
You may elect to transfer the files via the SCP (encrypted) or by FTP (non-encrypted) method. Please note, however, that if you set an file transfer method here, that method will be overridden if you later select a different method when transferring files manually from secondary "Show all files" windows. Click Submit to enter your changes.
Archive Information
Archive Method:
FTP
Host Name
User Name
Password
Confirm Password
Path
File Information:
Download
Transfer
File Name
Download
summary.log.ends20040917
summary.log.ends20040918
summary.log.ends20040919
summary.log.ends20040920
summary.log.ends20040921
summary.log.ends20040922
Submit
Reset
Back
Copyright © 2004, CipherTrust, Inc. All rights reserved.

When the **Show all files** hyperlink is clicked, a secondary browser window opens, displaying any Summary Log files that have not yet been deleted by IronMail's Cleanup Schedule. Enter Archive Information in the input fields at the top of the window, then select from the options below.

Download	This hyperlink opens a "Save As..." dialog allowing the Administrator to save the file to disk.
Transfer	If the **Transfer** check box is selected and Archive Information is provided in the input fields above, IronMail will automatically transfer the Summary Log file at the scheduled hour. Click **Submit** after selecting **Transfer** to save the user input.
File Name	This column identifies the names of the most recent files of the selected type. Because IronMail generates these files at approximately 12:30 AM, each day's Summary Log data does not become available for file transfer until the next morning.

Process ID Numbers

The Summary Log file displays an internal ID number used by IronMail to identify the many subsystems that can process a message. The Process ID is displayed in the second pipe-delimited field in the log. The table below maps the Process ID number to the process' name.

10	*	**165**	Nightly Schedule (running nightly scheduled tasks)
21	SMTPI Service	**166**	Statistics Collector
22	SMTPIS Service	**170**	Optimize
30	SMTPO Service	**180**	Mail-IDS
41	*POP3* Service	**190**	Anomaly Detection Engine
42	POP3S Service	**200**	Anti-Virus Queue
51	*IMAP4* Service	**210**	Content Filtering Queue
52	IMAP4S Service	**220**	Mail Monitoring Queue
90	Apache Web Server	**230**	Rip Queue
91	IronWebMail	**240**	Join Queue
100	Tomcat (JavaScript Interpreter)	**250**	Quarantine Queue
110	Admin (internal service that runs scripts)	**260**	Spam Queue
120	Alert Manager	**270**	SSH Command Line Interface
130	Cleanup Schedule	**280**	SSH Maintenance (monitoring the SSH port)
140	Health Monitor	**290**	Secure Web Delivery Queue
150	Report Generator	**300**	Audit
151	*Policy* Configuration	**330**	Bootport
160	Schedule (running periodic scheduled tasks)	**340**	Verity File Translator Queue
161	Schedule for FTP	**900**	Check Tool
163	Archive	**910**	Updater
164	LDAP Synchronization		

Queue IDs

IronMail's Queue Services (e.g., Mail Monitoring Queue, Anti-Spam Queue, etc.) are identified by numbers in Detailed Logs.

1	Anti-Virus Queue (AVQ)
2	Content Filtering Queue (CFQ)
3	Mail Monitoring Queue (MMQ)
4	Outbound Queue (SMTPO)
5	Rip Queue (RIPQ)
6	Join Queue (JOINQ)

8	Anti-Spam Queue (SPAMQ)
10	Secure Web Delivery Queue (SWMQ)
11	Verification (Extraction) Queue (VFQ)

Feature IDs

Some of IronMail's log files will report a numeric value representing a program "feature"—i.e. a broad program area in IronMail. The table below maps the feature ID number with its program area.

1	Mail-Firewall
2	Mail-VPN
3	IronWebMail
4	Mail-IDS
5	Anti-Virus
6	Policy Manager
7	Anti-Spam
9	Secure Delivery
10	Software/File Updates
11	*Centralized Management Console*

Sub-feature IDs

Some of IronMail's log files will report a numeric value representing a "sub-feature"—i.e. category of—IronMail's Policy Manager. The table below maps the sub-feature ID number with its policy category.

***Rule* Type**		
	0	System-generated rule
	1	User-generated rule
Sub-feature ID		
	1	Mail Monitoring
	2	Encrypted Message Filtering
	3	Off-Hour Delivery
	4	Attachment Filtering
	5	Content Filtering

	6	Message Stamping
User List Type		
	0	Email address
	1	Group
User Included		
	1	Included
	0	Excluded
Default Action		
	1	Pass through
	4	Drop part
Parts to scan		
	1	Body
	2	Attachments
	0	Both body and attachments
Message Direction		
	0	Inbound
	1	Outbound
	2	Both inbound and outbound

Default Action

IronMail's Attachment Filtering and Encrypted Message Filtering policies both include a "default action" value. These show up in Detailed Logs as numeric values. The table below maps the default action number with the specific actions.

For Attachment Filtering policies	
1	pass through
2	drop part
For Encrypted Message Filtering policies	
1	Drop encrypted message
2	Drop plain message
3	Quarantine encrypted message
4	Quarantine plain message

5	Allow encrypted message
6	Allow plain message

Message Delivery Modes

Some of IronMail's log files will report how messages were delivered.

0	Normal (non-secure SMTP delivery)
1	TLS
2	S/*MIME*
3	PGP
4	Secure Web Delivery
5	Deny TLS

Message Types

IronMail generates many notification emails to the administrator. These notifications are identified as numbers in IronMail's logs.

0	Normal
1	Notification (when an IronMail policy is enforced)
2	Forwarded (when an email is forwarded as a result of a policy)
3	Copied (when an email is copied as a result of a policy)
4	DSN (delivery status notification when IronMail cannot deliver a message)
5	SWM (notification to a recipient that an email may be read securely via the Secure Web Delivery mechanism)
6	Reports (email that IronMail generates containing Daily Reports)
7	EUSR_OUT (when Ironmail delivers End User Spam Reporting data to CipherTrust's "Global Collector)
8	EST_OUT (when IronMail delivers Enterprise Spam Reporting data to CipherTrust's "Global Collector)
9	EUSR_IN (messages that End User Spam Reporters forward to IronMail)
10	EST _ IN (messages that spammers send to the Enterprise Spam

	Reporting address)
11	Secure (messages that are encrypted with *SSL*, PGP, or S/MIME)
12	FWD_ATTACH (when IronMail forwards an email as an attachment)

Anti-Spam Tool IDs

Each of IronMail's spam-blocking tools are identified as numbers in the Spam Queue detailed log.

1	Reverse DNS
2	Realtime Blackhole List
3	Statistical Lookup Service
5	System Defined Header Analysis
6	User Defined Header Analysis
7	User Spam Reporting
8	Enterprise Spam Reporting
9	Enterprise Spam Profiler

Summary Log Actions

IronMail's Summary Log uses the following numeric codes to indicate specific actions it takes on messages.

100	No action
101	Multiple actions
102	Drop message
103	Drop part
104	Forward as attachment
105	Forward
106	Copy as attachment
107	Copy
108	Quarantine
109	Log
110	Rewrite Subject
111	Re-route
112	Encrypt
113	Change part

114	Add header
115	Retry message

Message Lock Values

Each email processed within IronMail's SMTPO Service (the Outbound Queue) can have one of 8 "states" or "statuses":

-1	Message has not yet been picked up for delivery
0	Message has been picked up for processing
1	SMTPO has opened connection to the receiving server to deliver the message
2	SMTPO is in the process of delivering message data
4	Message has been successfully delivered
5	SMTPO dropped the message because it could not be delivered
7	SMTPO dropped the message because of IronMail administrator intervention
8	SMTPO delivered the message to the Secure Web Delivery Server

Message Status Values

At any given time, a message may be in any of 4 stages of being processed

0	The message is on disk, but not currently being processed by any mail-processing subsystem
1	The message has been picked up by a mail-processing subsystem and is currently being processed
2	The message has been successfully delivered off IronMail
3	The message was dropped by IronMail

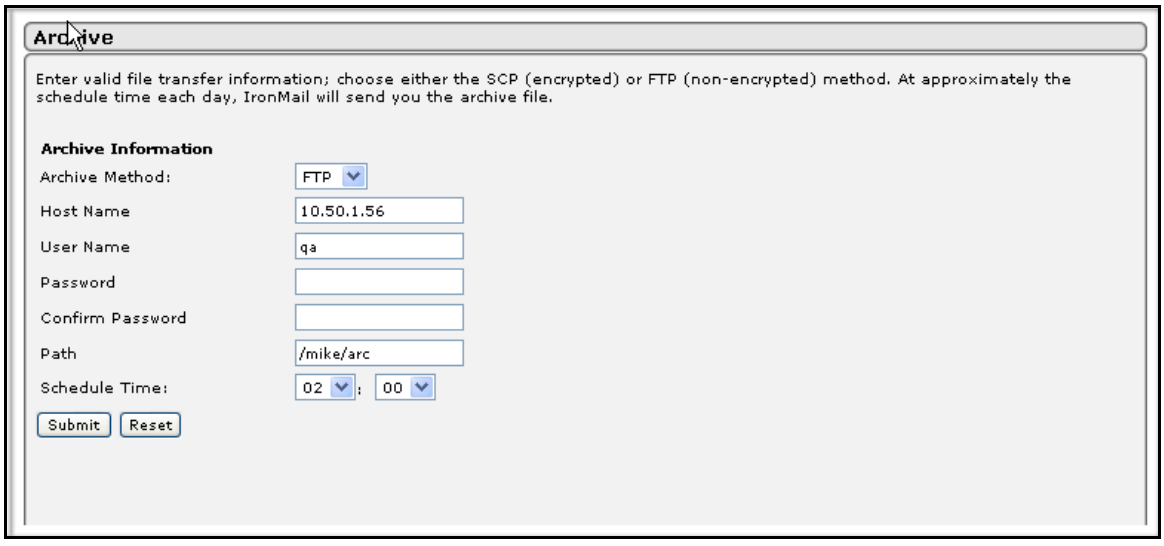
Static Rule IDs

Rules are created via a variety of mechanisms.

1	Rules created by End User Spam Reporting when in "manual" mode
2	Mail Monitoring rules created by the Anomaly Detection Engine
3	Attachment Filtering rules created by the Anomaly Detection Engine
4	Rules created by End User Spam Reporting when in "auto" mode
5	Rules created by Enterprise Spam Reporting when in "auto" mode
6	Rules created by Enterprise Spam Reporting when in "manual" mode
7	Rules pertaining to IP addresses created by the Anomaly Detection Engine

Archive

If IronMail's Archive Messages option is enabled (*Mail-Firewall > Configure Mail Services > "Global" hyperlink*), IronMail will save a copy of all inbound and outbound messages to disk. At approximately midnight, when IronMail generates its daily reports and log files, it will create a zipped file of all the day's messages. IronMail may then transfer them via SCP or FTP to a destination server at the time of day specified on this page.

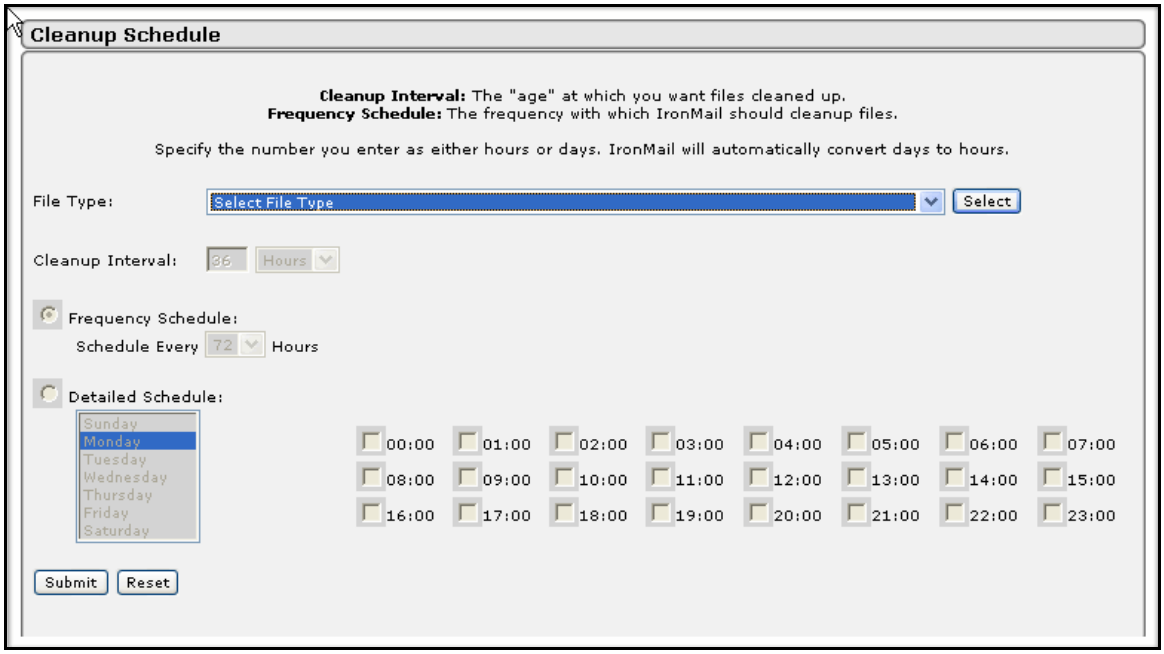


Note that IronMail only saves the tar file on disk for 24 hours. The next midnight, it deletes the tar file of archived messages.

Archive Method	Select an archive method IronMail should use when transferring the archived messages tar file: • **SCP:** Select SCP to transfer the file securely using the SCP *protocol*. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files to the same directory, earlier files will be over-written with later IronMail transfers.
Host Name	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.
Password	Enter and confirm a valid password.
Path	Enter the path string to the location on the archive server where IronMail should transfer the file. **Note:** the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the file.

Cleanup Schedule

IronMail accumulates many files and data over time. We recommend that you allow IronMail to regularly purge the system of unnecessary files and data. Navigate to *Administration > Cleanup Schedule* to reach the screen below.



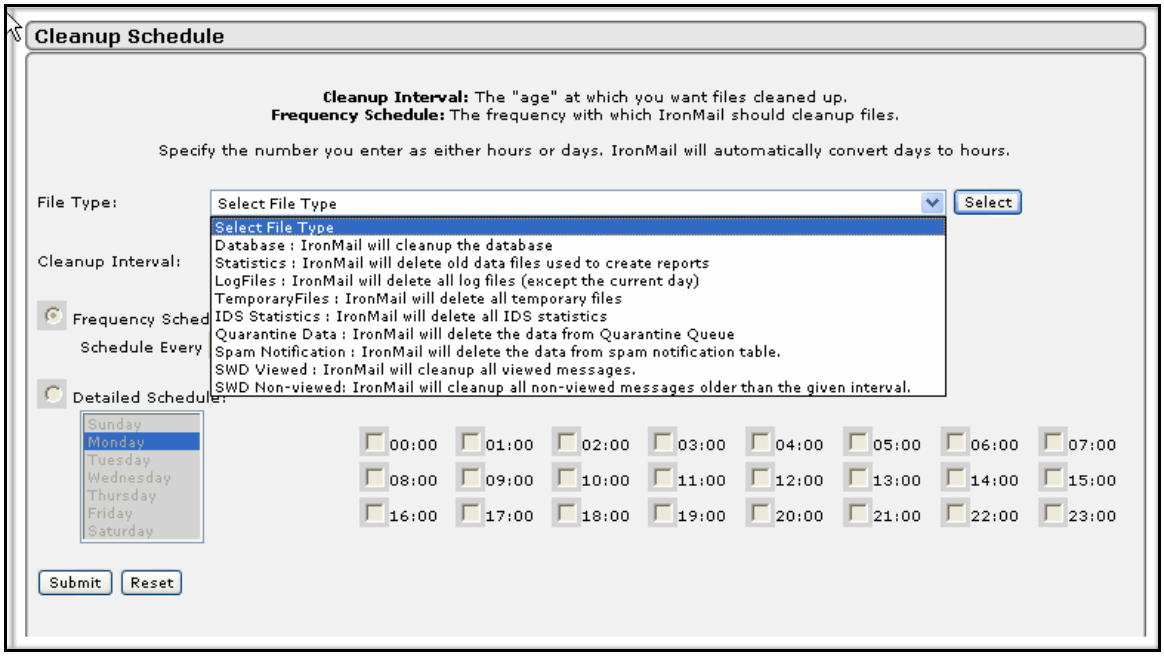
Administrators must specify three options:

- The file to be cleaned;
- The Cleanup Interval - or, how long a file may remain on disk. When the cleanup process runs at the specified frequency or detailed schedule, it will look for and delete files that have remained on disk this long or longer.
- A Cleanup Cycle - how often IronMail runs Cleanup. This cycle may be either a Frequency Schedule or the Detailed Schedule configured on this screen.

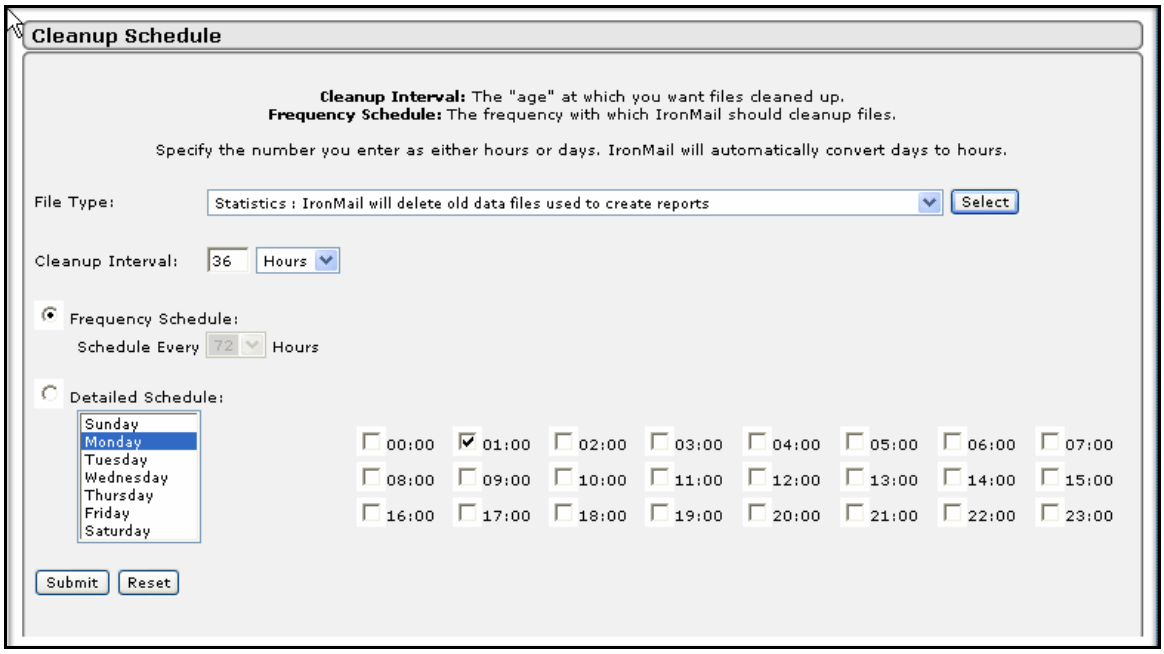
Field	Description
File Type	From the pick, select the type of file for which you are scheduling cleanup. Options are: • Database • Statistics • Log Files • Temporary Files • IDS Statistics • Quarantine Data • Spam Notification • SWD Viewed • SWD Non-viewed

Cleanup Interval	Specify the number of hours or days (enter the number and select from the pick list) that the particular kind of file should remain in the database. IronMail converts a "days" entry into hours internally.
Frequency Schedule **or** **Detailed Schedule**	If you want to simply set an interval between cleanup cycles, click the Frequency Schedule radio button and select the number of hours between cleanup runs. If you prefer to set specific days and times for cleanup, click the Detailed Schedule radio button, then select a day to configure and click the checkbox(es) beside the time(s) of day when cleanup should occur. You must set each day separately, since IronMail will not support selecting multiple days at one time.

The two screen shots that follow illustrate the configuration process in greater detail.


Cleanup Schedule
Cleanup Interval: The "age" at which you want files cleaned up.
Frequency Schedule: The frequency with which IronMail should cleanup files.
Specify the number you enter as either hours or days. IronMail will automatically convert days to hours.
File Type:
Select File Type
Select
Select File Type
Database : IronMail will cleanup the database
Statistics : IronMail will delete old data files used to create reports
LogFiles : IronMail will delete all log files (except the current day)
TemporaryFiles : IronMail will delete all temporary files
IDS Statistics : IronMail will delete all IDS statistics
Quarantine Data : IronMail will delete the data from Quarantine Queue
Spam Notification : IronMail will delete the data from spam notification table.
SWD Viewed : IronMail will cleanup all viewed messages.
SWD Non-viewed: IronMail will cleanup all non-viewed messages older than the given interval.
Cleanup Interval:
Frequency Sched
Schedule Every
Detailed Schedule:
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00
08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00
16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00
Submit
Reset

The screen above shows the list of file types, and the one below illustrates interval and schedule options.



In most cases, administrators will want to keep a "rolling window" of data on IronMail's hard disk. A "rolling window" is created when, for example, at any given time, there are three days' worth of data on disk. That is, once a day, IronMail deletes files or data older than three days. To create rolling windows, the cycle time should always be *less* than the cleanup interval.

If the cleanup interval is shorter than the cycle time - for example, a cleanup interval of 1 hour and cleanup cycle of 24 hours - at each cleanup interval, 23 hours worth of the specified data is deleted.

Configure Mail Certificates

This screen is used to select the X.509 Certificate IronMail will use for SSL encryption. All installed X.509 certificates will show on the pick list. The Administrator selects one from the pick list and clicks **Submit**.

onfigure Certificate
All X.509 Security Certificates that have been installed on IronMail appear in the pick list. Select the one IronMail should use for SSL encryption of SMTP, POP3, and IMAP4 email. ("Default" in this list refers to the invalid certificate that is installed by default to allow for Web Administration.)
Select Certificate:
DEFAULT
Submit
Reset

Although this function may be logically seen as part of Certificate Management, the screen is actually located under Administration (Administration > Configure Mail Certificates).

Web Administration

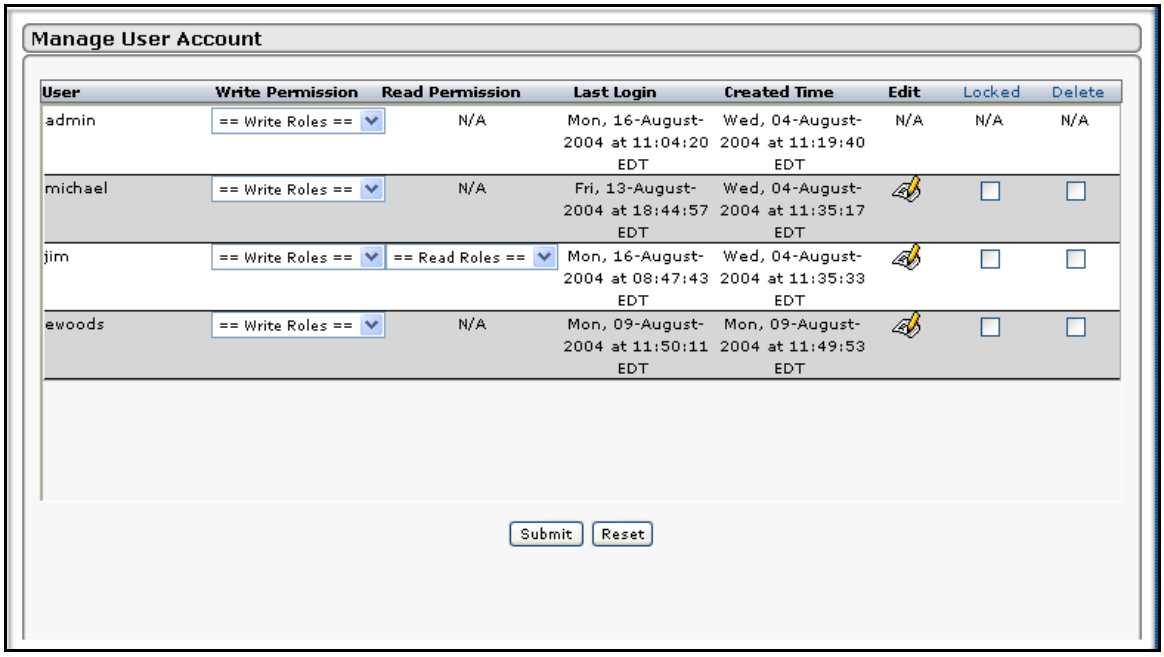
User Accounts

The IronMail administrator may create user accounts for additional personnel who are granted permission to perform specific duties in administering the IronMail appliance. The administrator can select which program areas users are allowed to access, and whether their access is "read only" or "read/write."

There is one "super user" account for the IronMail administrator. This "super user" account name is "admin." Only the admin user account has access to this User Accounts window.

IronMail generates a daily log (*Monitoring > Reports/Log Files > Detailed Log Files > "Audit.log"*) showing each users' login and the IronMail windows they accessed.

The Manage User Accounts link on the main IronMail page opens a screen that displays all existing user accounts for the specific appliance.



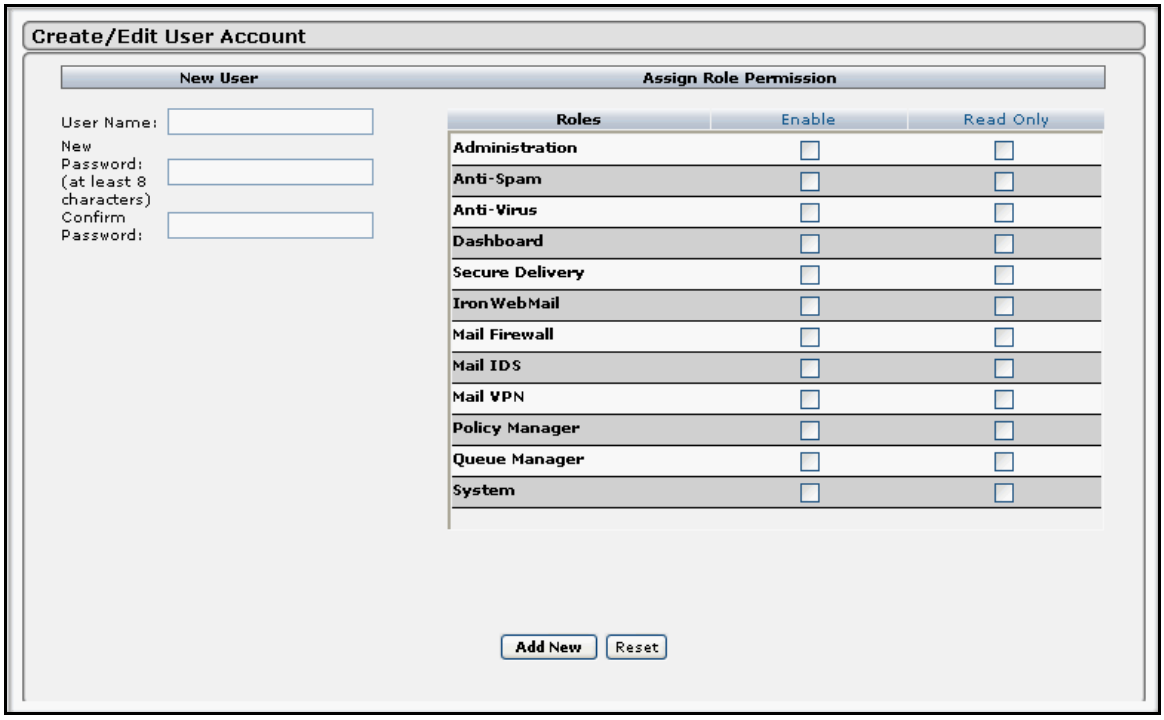
A table of user accounts is displayed. The table shows the logon name and program permissions for each user account. (Until user accounts are created, only the "admin" super-user account is displayed.) The table of User Accounts displays the following information:

User	This column displays the usernames of personnel granted access to the IronMail.
Write Role	This column displays a dropdown list for each user account showing the program areas for which he or she has been granted "read/write" permission.
Read Role	This column displays a dropdown list for each user account showing the program areas for which he or she has been granted "read only" permission.
Last Login	This column shows the day, date and time of the last login for the associated user ID.
Created Time	The column displays the day, date and time of creation for the associated ID.

Edit	To change the program permissions for a user, click **Edit**. The username and current program permissions are displayed in the Edit User table at the bottom of the page. Select or deselect read-only or read/write check boxes as required, and click **Submit** to save the input. The Admin ID cannot be edited,locked or deleted.
Locked	Click the Locked checkbox for any user whose access to IronMail should be temporarily blocked. A disabled account can neither access the Web Administration nor Command Line Interface. Uncheck the box to enable the account.
Delete	Click **Delete** to permanently remove a user account from IronMail.

Creating or Editing a User Account

The Create Account hyperlink for new accounts or clicking the Edit icon for existing accounts opens the Create/Edit User Account screen. For existing accounts, the configuration options will be pre-populated.

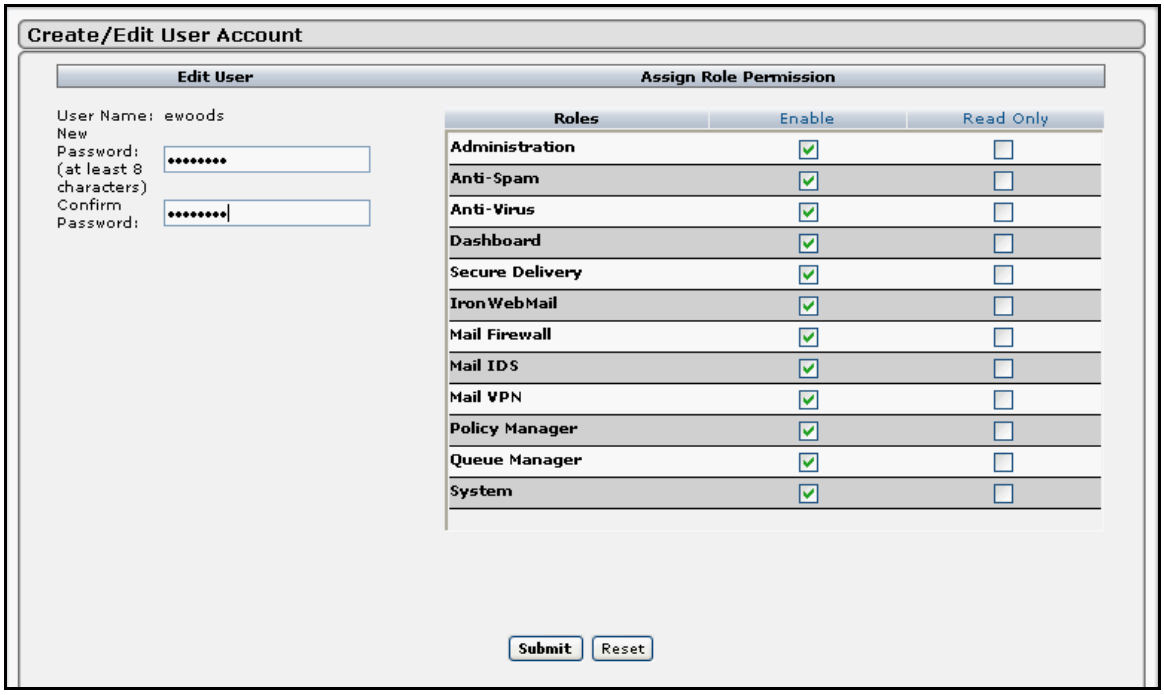


Input fields allow the creation or editing of user accounts.

User Name	Enter a logon name to the IronMail appliance. The username may be up to 54 characters, and is case insensitive. The username (and password) allows access to both the graphical and command line interface to IronMail.
Password	Enter a temporary password. (Passwords allowing access to IronMail should be "strong"—that is, a combination of alphanumeric characters, with upper and lower case and special characters.) The password must be at least 8 characters in length. The user may change the temporary password at his or her first logon by navigating to *System > Change Password.*
Confirm Password	Enter the password again to verify spelling.

Roles	The "Role" column identifies each of IronMail's program areas, as represented by the top level navigation tabs at the top of the Web Administration interface.
Enable	The check boxes in the Enable column allow read/write access to the individual program areas. The tab for any program area disappears from the Web Administration interface for any function that is not selected here or in the Read Only column. Clicking the **Enable** column heading hyperlink selects or deselects all program areas.
Read Only	The check boxes in the Read Only column allow "read only" access to a selected program area. Users with "read only" access may access the selected program areas within the Web Administration interface, and view all the data displayed within them, but the **Submit** button has been removed preventing any modification of appliance and *policy* settings and configuration. Note: selecting a **Read Only** check box also places a mark in the **Enable** check box. Even though the **Enable** check box is marked, the user has "read only" access to that program area. Clicking the **Read Only** column heading selects or deselects all program areas.

The completed screen for an account should appear like the one below.



Users may be assigned combinations of "read/write" and "read only" permissions.

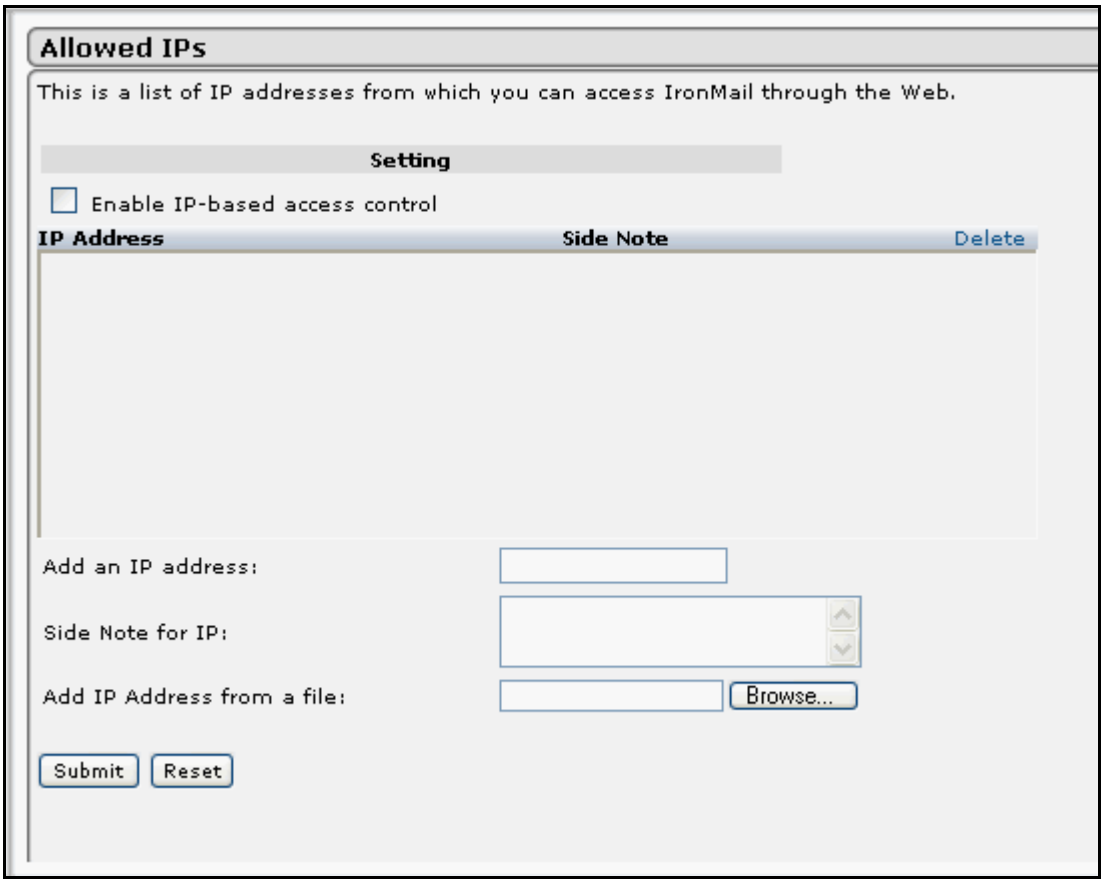
Depending on if a user account is being added or edited, click **Submit** to save the input.

Allowed IPs

If the "Allowed IPs" option is enabled, IronMail will only accept browser connections (for Web Administration) from workstations or laptops with the IP addresses specified in the table on this page. (If this option is not enabled, IronMail administrators may logon from any workstation.)

Warning! If "IP-based access control" (*ACL*) is enabled without entering valid IP addresses (i.e. addresses from which administrators may connect to IronMail), all IronMail administrators will be immediately locked out of the Web Administration interface.

Administrators must logon to IronMail's Command Line Interface, either from an SSH client or via a keyboard and monitor attached to the appliance, and disable this setting. (The CLI command to disable IP-based access control is: "system restore acl" (see the "System" commands in Command Line Interface).



The table of IP addresses displays the following information:

IP Address	This column displays IP addresses allowed to access IronMail's Web Administration interface.
Side Note	This column displays any notes an administrator may have provided to "identify" to whom or where the IP address belongs.
Delete	Select an IP address' **Delete** check box and click **Submit** to delete an address from this table.

Three input fields below the table of IP addresses allow the addition of IP addresses to the ACL list.

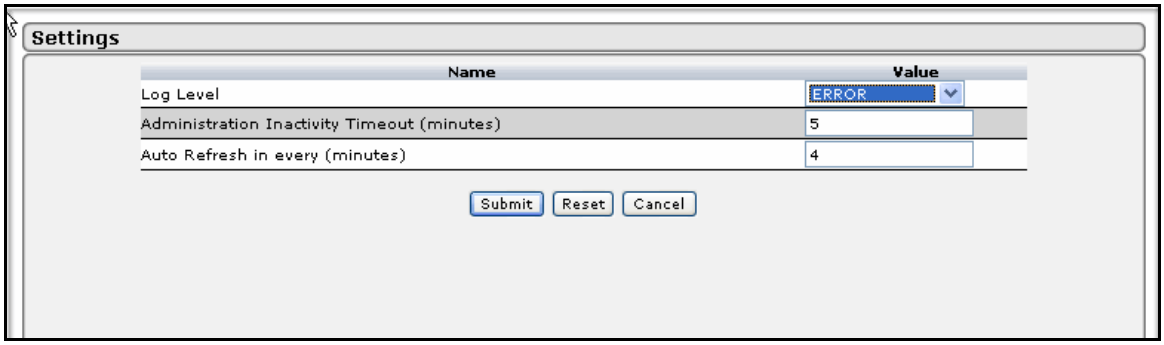
Add an IP address	Enter an IP address. Subnets are not allowed.
Side Note for IP	Provide any text that may help identify or describe the IP address.
Add IP Address from a file	If a list of IP addresses already exists in a text file, they may be imported in one step, rather than being entered individually. The addresses must reside in a plain ASCII text file. Each address must appear on a separate line. **Browse** to the text file and click **Submit**.

Enter IP addresses for machines that may connect to IronMail's Web Administration interface and click **Submit**. Repeat for as many machines as desired.

Configure

The primary interface to the IronMail appliance is through a secure web browser session. IronMail is best administered through Microsoft Internet Explorer (IE) version 6.0 or higher. Earlier versions of IE are capable of generating idiosyncratic anomalous behaviors depending on the system-configuration of the PC from which it is being run. The UNIX version of Netscape Navigator version 4.79 is the only other web browser CipherTrust supports, though there are significant known compatibility issues with that browser.

IronMail offers several configuration options related to the graphical Web Administration interface.



Log Level	IronMail generates a Web Admin log recording the activities of users who access the Web Administration interface. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the amount of detail written to the log. Select a value from the pick list.
Administration Inactivity Timeout	IronMail automatically logs out an administrator after a period of inactivity. (Web Administration sessions are "cookie-based"—each time an administrator performs an action within the graphical interface, IronMail queries and updates the timestamp on the cookie.) Enter a number, from one to thirty, representing how many minutes of inactivity may elapse before IronMail forces an administrator to log back into the graphical interface. Note that a change in the administrative inactivity timeout does not take effect until after an administrator logs out and logs back in again.
Auto Refresh in every (minutes)	IronMail can automatically refresh all pages that contain dynamic data, (e.g., *Queue Manager > Queue Information*, *Mail-IDS > Application Level > DoS Protection*, and *Dashboard*). Enter a number of minutes, from 1 to 29. IronMail will display text at the bottom of all pages that contain dynamic data indicating the frequency of the Refresh Rate. A change in the auto refresh does not take effect until after an administrator logs out and logs back in again. Note that Auto Refresh will *release* queues that have been *paused*. (IronMail automatically stops a queue from processing messages when an administrator opens a queue's Message Header Detail window. The queue remains paused as long as the window is open or five minutes of inactivity lapse.) Administrators should be aware, therefore, that if they expect to perform email management within a queue, a short Auto Refresh rate may impact their ability to process those messages.

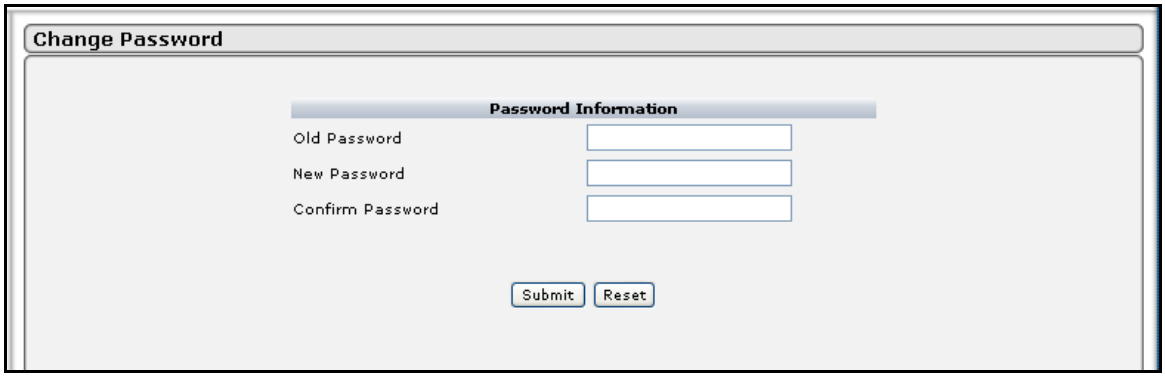
Known Browser Issues

The UNIX version of Netscape Navigator version 4.79 causes the following irregularities to be experienced when administering the IronMail appliance:

- **Mail-IDS > Vulnerability Assessment:** Vulnerability Assessment does not allow the entry of a hostname for report generation. Using an *IP address* works correctly. Future versions of IronMail have removed the acceptance of a hostname.
- **Mail-Firewall > Mail Routing > Domain-based:** Unable to enter valid mail routing domain information. There is an obvious error for domain validation. When entering a valid *domain name* and machine name, an invalid domain name error message will appear.
- **Queue Manager > Configure Queues > Change/Remove Queues:** Cannot click the **Submit** button on the Configure Queues screen. When attempted, an error message is displayed that reads "Duplicate Spam positions." This error message is incorrect, because there are no duplicate position entries. Administrators will have to use IE to configure this screen.
- **Anti-Spam >Spam Order:** Cannot click **Submit** on the Spam Order screen. When attempted, an error message is displayed that reads "Duplicate Spam positions." This error message is incorrect because there are no duplicate position entries. Administrators will have to use IE to configure this screen.
- ***Policy*** **Manager > Mail Monitoring > Apply Rules:** The **Delete** check boxes are mis-aligned on the Mail Monitoring *Rule* Application screen. The **Delete** check boxes appear below the System heading.
- **Anti-Spam > All screens:** Input validation is not correctly performed. Invalid data is allowed to be submitted.
- **Installation Wizard:** The keyboard's **Enter** key does not consistently work when submitting data on some screens. The screens where the **Enter** key did not submit the entered data were Steps 4, 6, 7, 8 and 9.

Change Password

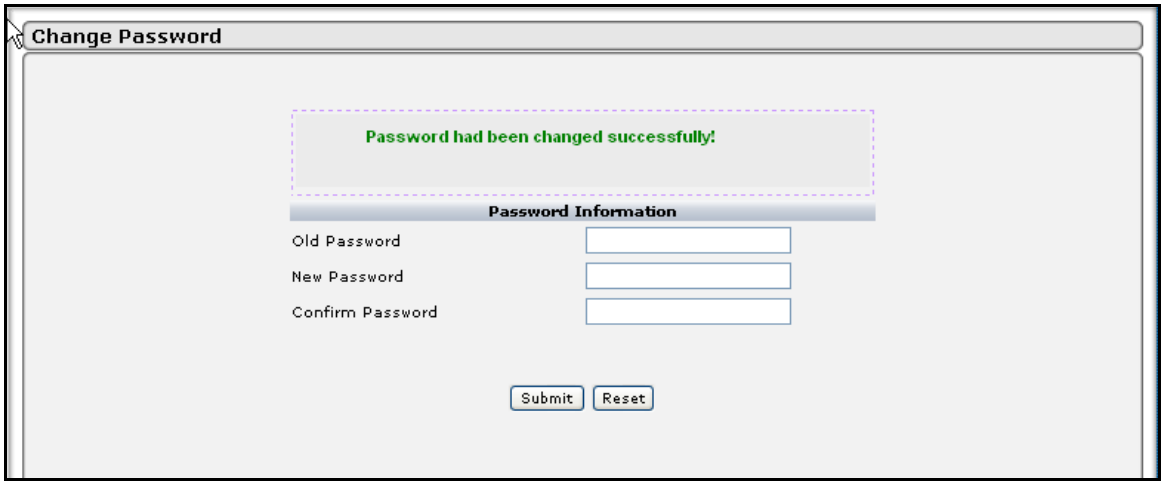
Administrators are strongly encouraged to change the default “admin” password (“password”) during their first administrative session with IronMail. Thereafter, the password may be changed at any time.



Old Password	Enter the old password.
New Password	Enter a new password. (Passwords may be between 8 and 20 characters in length, and may be alphanumeric. Passwords are case sensitive.)
Confirm Password	Enter the new password a second time to verify it.

Click **Submit** to save the new password.

Note that while the “admin” password may be changed at any time, the “admin” username may not be changed or deleted—it is always “admin.”



System Functions

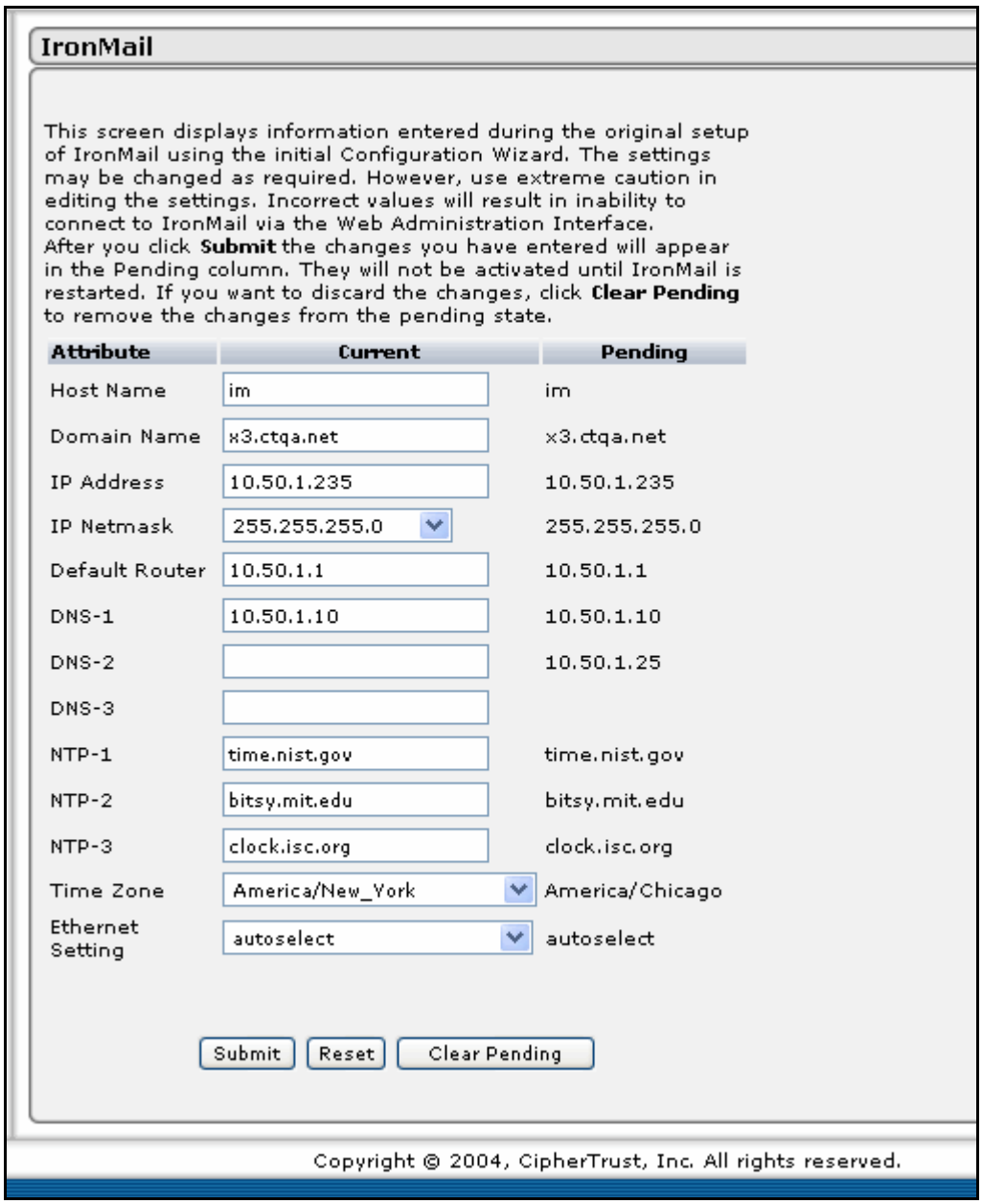
Configuring the System

Configuration

The Configuration program area is used to change settings related to the IronMail appliance itself. The **Configure** hyperlink expands to offer IronMail, Out-of Band Management, Routing, Serial Port, SSH Configuration, Backup, Restore, and Check Tool sub-menus.

IronMail

Initially, the Configure IronMail page displays information that was entered during the Initial Configuration Wizard when IronMail was first installed. At any time afterward, these settings may be changed as required.



Host Name	Enter a "host name" for the IronMail appliance. The host name must be entered in all lower-case letters for IronMail's Backup and Restore utilities to function correctly. This name must be resolved in DNS.
Domain Name	Enter the domain name to which IronMail belongs.
IP Address	Enter IronMail's IP address. (The host name and IP address must be resolved in DNS.)
IP NetMask	Enter the *subnet* mask required by the IP address.
Default Router	Enter the IP address of the default router.
DNS-1	Enter the IP address of the primary *DNS server*. (At least one DNS server must be provided.)
DNS-2	Enter the IP address of a secondary DNS server. (A second DNS server is optional.)
DNS-3	Enter the IP address of a tertiary DNS server. (A tertiary DNS server is optional.)
NTP-1	Enter the fully qualified domain name of a Network Time Protocol time server. IronMail will synchronize its internal system clock with this server. IronMail will query the NTP server once every minute. It the NTP server is unavailable, IronMail will query a secondary and tertiary NTP server if their names are provided immediately below.
NTP-2	Enter the fully qualified name of a secondary NTP server. IronMail uses this only as a backup if the first NTP server cannot be reached. IronMail does not "average" the time between multiple time servers.
NTP-3	Enter the fully qualified name of a tertiary NTP server. IronMail uses this only as a backup if the first and second NTP servers cannot be reached. IronMail does not "average" the time among multiple time servers.
Time Zone	Select from the **Time Zone** pick list a city that belongs to the same time zone where IronMail is located.
Ethernet Settings	"Ethernet Settings" was not part of the Initial Configuration Wizard. Use this setting to resolve network difficulty that may be experienced when IronMail is physically connected to a network router or switch. While most hardware is designed to automatically negotiate an Ethernet "handshake," and agree on a speed and duplex mode, auto-negotiation is not always successful. Administrators must know the specific Ethernet settings of the hardware to which IronMail is physically connected. Select from IronMail's **Ethernet Settings** pick list a matching configuration. The Ethernet setting by default is "Autoselect." You may set it for the other available settings as required. However, should IronMail display erratic behavior with large files (>100kB), return the Ethernet Setting to "Autoselect."

As the table above shows, the Administrator has the capability to select the interface speed to be used when IronMail connects to a network. For specific appliances (IronMail 305 and IronMail 345 series) the system supports Gig Ethernet connection, allowing higher performance in some applications. Gig Ethernet is capable of data transmissions over a local area network (LAN) at a rate of up to 1.25 gigabits per second; however, IronMail is an SMTP email gateway; users will not gain full advantage of that capability because email messages do not involve large data packets. Email traffic is burst-oriented, rather than consisting of long data strings.

Regardless of the model of appliance, only the settings supported by that appliance are displayed on the screen. Supported configuration options are shown in the table below:

Appliance	Interface(s)	Ethernet Configuration Options
IronMail 112	**fxp** - using the Intel EtherExpress Pro/100B Ethernet device driver	autoselect - enables automatic selection of the media type (see below) and options supported 10baseT/UTP (full duplex) - enables 10Mbps operation 100baseTX (full duplex) - enables 100Mbps operation
IronMail 305	**bge** - using the Intel (R) Pro/1000 gigabit Ethernet driver	autoselect - enables autoselection of the media type and options supported 10baseT/UTP - enables 10Mbps operation in half duplex mode. 10baseT/UTP (full duplex) - enables 10Mbps operation 100baseTX - enables 100Mbps operation in half duplex mode 100baseTX (full duplex) - enables 100Mbps operation 1000baseTX - enables 1000Mbps operation over twisted pairs; only full duplex mode is supported.
IronMail 345 series	**em** - using the Broadcom BCM570x PCI gigabit Ethernet adaptive driver	autoselect - enables autoselection of the media type and options supported 10baseT/UTP - enables 10Mbps operation in half duplex mode 10baseT/UTP (full duplex) - enables 10Mbps operation 100baseTX - enables 100Mbps operation in half duplex mode 100baseTX (full duplex) enables 100Mbps operation 1000baseTX - enables 1000Mbps operation over twisted pairs; only full duplex operation is supported

The media type mentioned in the table above will be one of two options:

- half duplex - the system uses only one twisted pair of wires, essentially limiting message transmission to one direction at a time. The particular connection can be sending (outbound message) or receiving (inbound message) but not both at the same time.

- full duplex - the system uses two twisted pairs of wires simultaneously, allowing messages to flow in both directions at once.

CiphterTrust recommends choosing the autoselect configuration, since that choice allows the system to select the best option at any time.

After entering new values and clicking **Submit**, the new values are displayed in the **Pending** column to the right of the user input fields. The pending changes will not take effect until IronMail is restarted.

Use extreme caution when editing the IP address, Subnet, or Gateway values. Incorrect values will result in inability to connect to IronMail via the browser Web Administration interface.

Restoring Default Network Settings

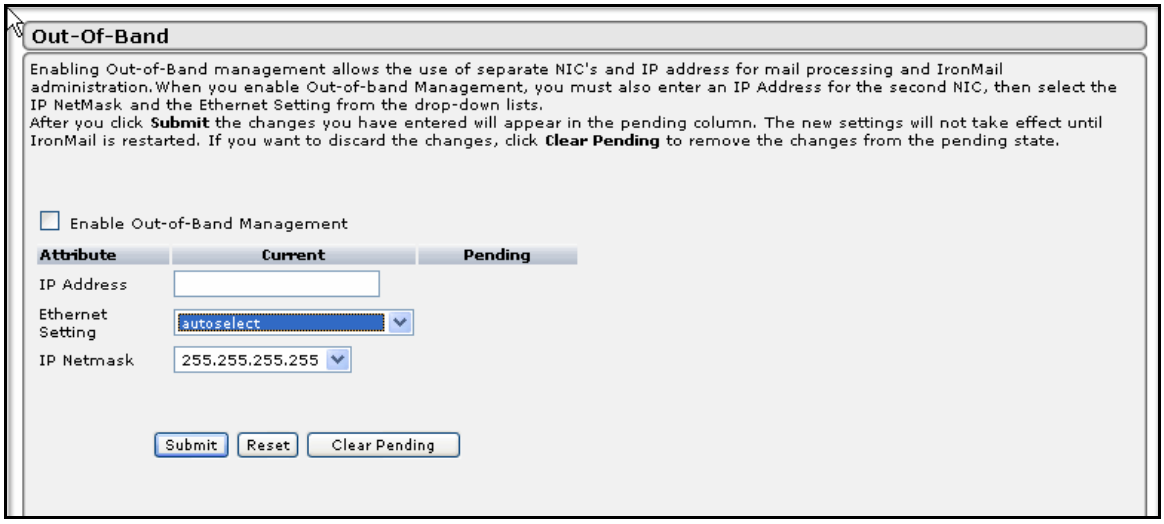
If network settings are entered incorrectly, physically connect to the IronMail via keyboard and monitor (the keyboard must be plugged into IronMail's serial port before the appliance is powered on). Log onto IronMail's command line interface using the same username and password used in the Web Administration interface. Use the CLI commands to reset IronMail to the factory default settings. Once the default settings are restored, the administrator may log back onto the Web Administration interface using the default IP address. He or she can then re-enter the correct network information. Note, however, that resetting IronMail to the factory default settings also resets all of its settings—routing, email *policy*, queue and mail service, etc.—to the factory default.

IronMail has a standard configuration of Maximum Transferred Unit (the maximum size for a single *packet* that may be transferred by the email system) of 1,500 bytes. If your system requires a maximum other than the standard MTU configuration, CipherTrust's Technical Support engineers can accomplish a custom configuration at your request.

Out-of-Band Management

Only configurable and visible in IronMail appliances containing two *network* interface cards (for example, the IronMail 345 series), this window allows administrators to use separate NICs and IP addresses for IronMail administration and mail processing. Email will flow through the first NIC, while Web Administration and Command Line management of the appliance occur on the second NIC. This allows management of the IronMail through a connection (out of band) that is not accessible to anyone using the normal email flow channels (in-band)

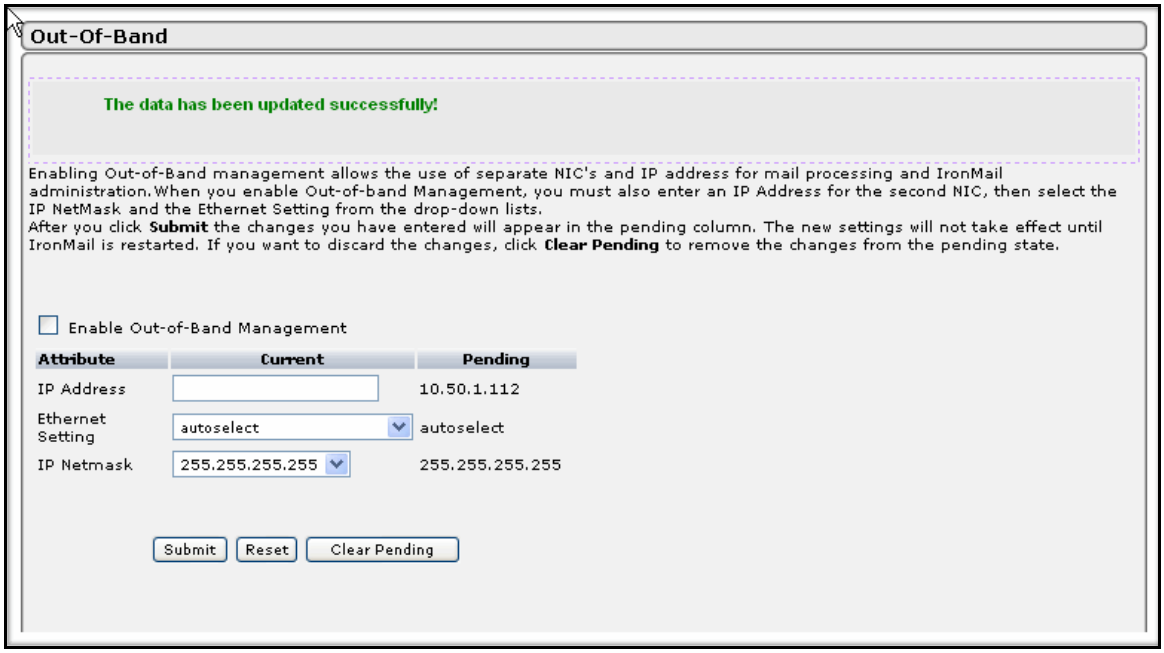
After the Initial Configuration Wizard reboots the IronMail appliance after the initial network settings are entered at the time of installation, the presence of a second NIC will be auto-detected and the administrator will be prompted to enter the network parameters of the additional card. (To ensure maximum security, the second NIC should not be placed on the same network segment as the internal mail server.) Use the input fields on this page to make subsequent changes to the second NICs network values.


Out-Of-Band
Enabling Out-of-Band management allows the use of separate NIC's and IP address for mail processing and IronMail administration. When you enable Out-of-band Management, you must also enter an IP Address for the second NIC, then select the IP NetMask and the Ethernet Setting from the drop-down lists.
After you click Submit the changes you have entered will appear in the pending column. The new settings will not take effect until IronMail is restarted. If you want to discard the changes, click Clear Pending to remove the changes from the pending state.
Enable Out-of-Band Management
Attribute
Current
Pending
IP Address
Ethernet Setting
autoselect
IP Netmask
255.255.255.255
Submit
Reset
Clear Pending

Field	Description
Enable Out-of-Band Management	This checkbox enables the use of separate NIC's for IronMail Administration and email flow. The information you will enter is for the *second* network interface card.

Attribute	*IP Address* - Enter the IP address for the second network interface card. IP NetMask - Select the appropriate netmask from the drop-down list. Ethernet Setting - Select the proper Ethernet setting from the list. You may choose to let the IronMail automatically select the appropriate setting, or choose from multiple options for 100baseTX or 10baseT.
Current	This column displays the current settings of the Attributes
Pending	This column displays revised settings you wish to enable. These settings will become Current settings when your submission is processed.
Buttons	Submit - Clicking this button submits your changes, placing all the reconfigured values in the Pending column. Reset - Returns the input fields to their previous values *before* any changes have been submitted. Clear Pending - Resets the input fields to their previous values *after* changes have been submitted, but *before* the appliance has been rebooted.

After entering and/or selecting the required values, click **Submit**. The data will display in the Pending column to the right of the input fields. The data does not "take effect" until the appliance is rebooted.


Out-Of-Band
The data has been updated successfully!
Enabling Out-of-Band management allows the use of separate NIC's and IP address for mail processing and IronMail administration. When you enable Out-of-band Management, you must also enter an IP Address for the second NIC, then select the IP NetMask and the Ethernet Setting from the drop-down lists.
After you click Submit the changes you have entered will appear in the pending column. The new settings will not take effect until IronMail is restarted. If you want to discard the changes, click Clear Pending to remove the changes from the pending state.
Enable Out-of-Band Management
Attribute
Current
Pending
IP Address
10.50.1.112
Ethernet Setting
autoselect
autoselect
IP Netmask
255.255.255.255
255.255.255.255
Submit
Reset
Clear Pending

Click **Clear Pending** to reset the input fields to their previous values.

Note: The IP address will be removed when Out-of-Band Management is disabled, in order to prevent it from remaining assigned, and therefore unavailable for reassignment.

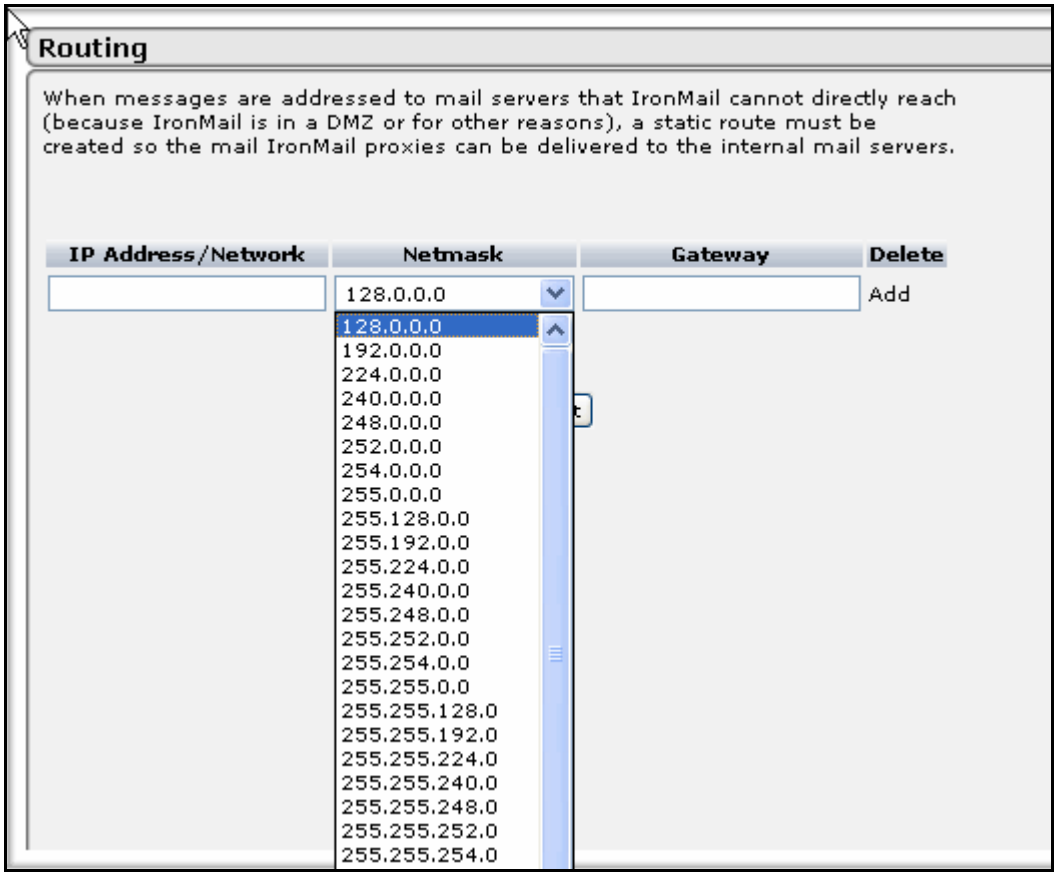
Anytime a change is made in the network configuration for this second NIC, the IronMail appliance must be rebooted (*System > Power Down/Restart.*)

When logging onto the IronMail Web Administration interface via the out-of-band NIC, the port number (:10443)-suffix is required in the URL, as illustrated here: https://10.50.1.xxx:10443.

When Out-of-Band is enabled, the IronMail's command line interface is only accessible through the IP address of the second NIC.

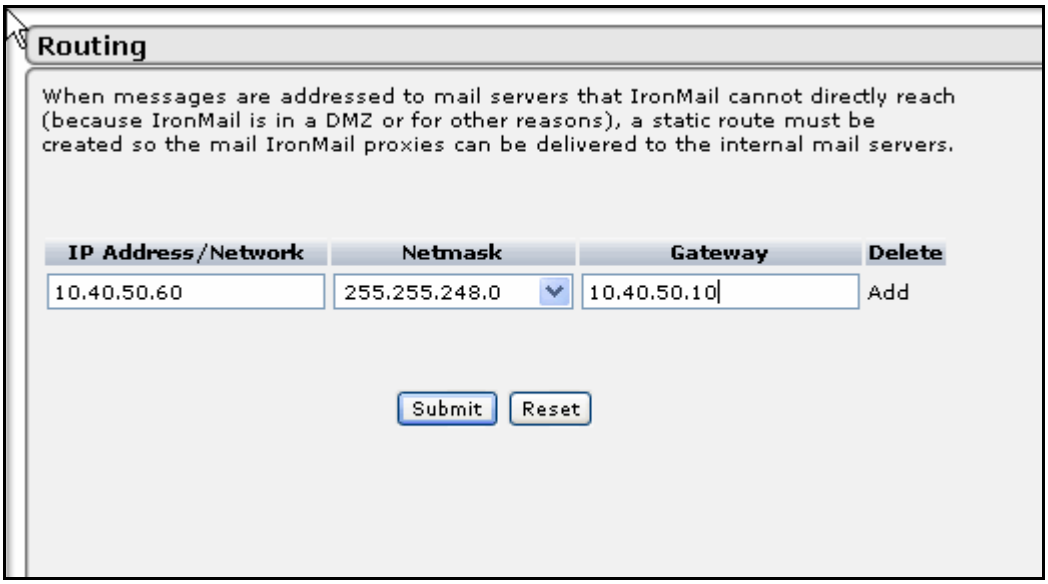
Routing

When messages are addressed to mail servers that IronMail cannot directly reach (because IronMail is in a *DMZ* or for other reasons), a static route must be created so the mail IronMail proxies can be delivered to the internal mail servers. The Routing screen allows the Administrator to create this route.

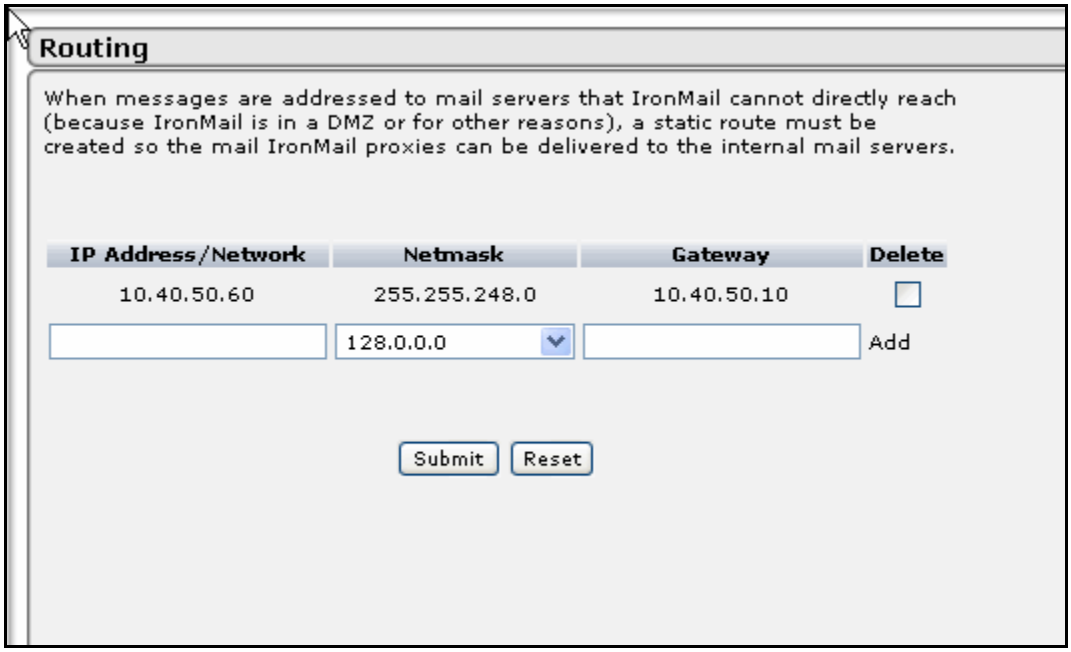


IP address*/*Network	Enter the IP address of the machine that IronMail must deliver its mail to.
NetMask	Select from the **NetMask** pick list the *subnet* mask used by the machine.
Gateway	Enter the IP address of the gateway that knows how to reach the machine IronMail needs to deliver its mail to.
Delete	Select a machine's **Delete** check box and click **Submit** to delete a "route" from this table.

To create the static route, enter or select the appropriate data, as shown below.


Routing
When messages are addressed to mail servers that IronMail cannot directly reach (because IronMail is in a DMZ or for other reasons), a static route must be created so the mail IronMail proxies can be delivered to the internal mail servers.
IP Address/Network
Netmask
Gateway
Delete
10.40.50.60
255.255.248.0
10.40.50.10
Add
Submit
Reset

Click **Submit** to record the configuration. The screen updates to show the route.

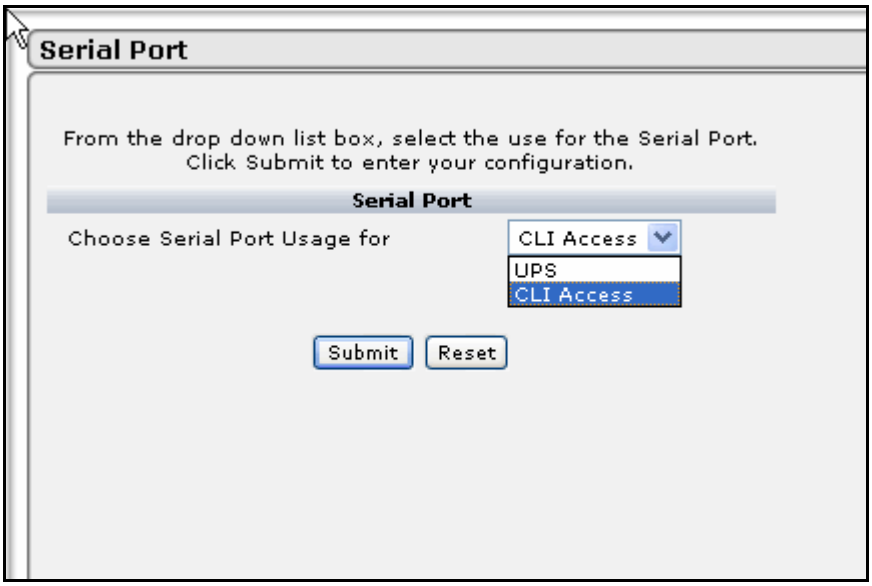

Routing
When messages are addressed to mail servers that IronMail cannot directly reach (because IronMail is in a DMZ or for other reasons), a static route must be created so the mail IronMail proxies can be delivered to the internal mail servers.
IP Address/Network
Netmask
Gateway
Delete
10.40.50.60
255.255.248.0
10.40.50.10
128.0.0.0
Add
Submit
Reset

IronMail must be rebooted before the static information in this table can be used.

The Serial Port

IronMail's serial port may be configured for either one of two possible uses:

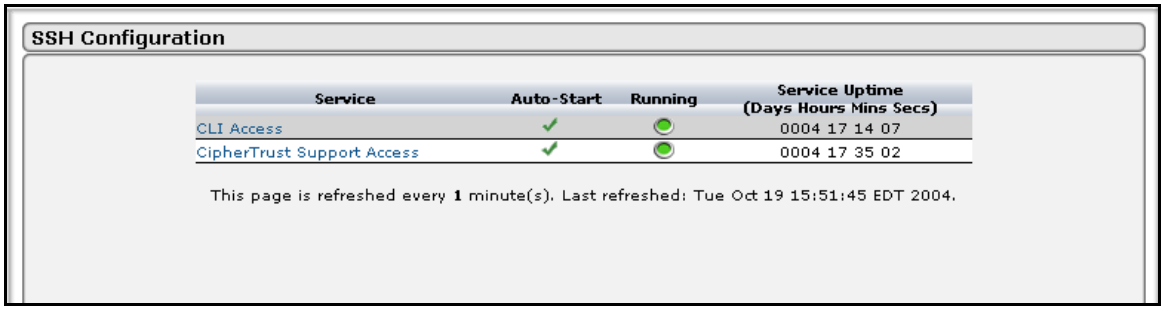
- as the connection port for an uninterruptable power supply, or
- as the access port for command line interface access using a keyboard (and monitor) connected directly to the IronMail appliance.



To configure the serial port, the Administrator must select the desired use from the pick list, then click **Submit** to record the selection.

SSH Configuration

Accessibility to IronMail's command line interface is controlled by the "CLI Access Service." If this subsystem is not running, administrators will be unable to log onto IronMail via their favorite SSH client.



The SSH Configuration table contains four columns: Service, Auto-Start, Running, and Service Uptime.

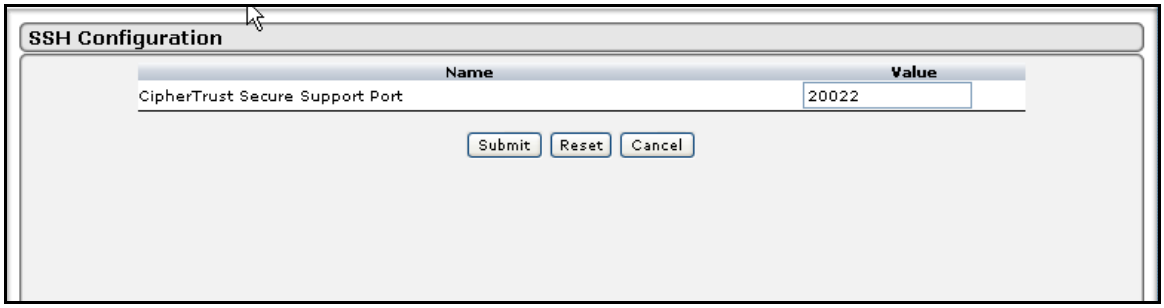
Service	This column identifies the "CLI Access" Service. Two services are configurable: • CLI Access - allows the Administrator to use the command line to control the IronMail appliance. • CipherTrust Support Access - gives the Support Engineers remote access to the customer's IronMail to enable Support to assist, help solve problems, etc. The service names are hyperlinks allowing the Administrator to configure available details about each service.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If the icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green IronMail's Health Monitor will restart a Service that has stopped for any reason when it performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot or when Health Monitor runs its system tests.

	(Note that a service can continue to run after its auto-start setting is turned off. A service cannot start running, however, until its auto-start setting is turned on.) The red and green icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from green to red, as expected. If the icon does not toggle, click the SSH Configuration hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted.

If the "uptime" appears less than expected, it may indicate that the service was manually stopped by an administrator or by an unexpected program error, but was restarted automatically by IronMail's Health Monitor.

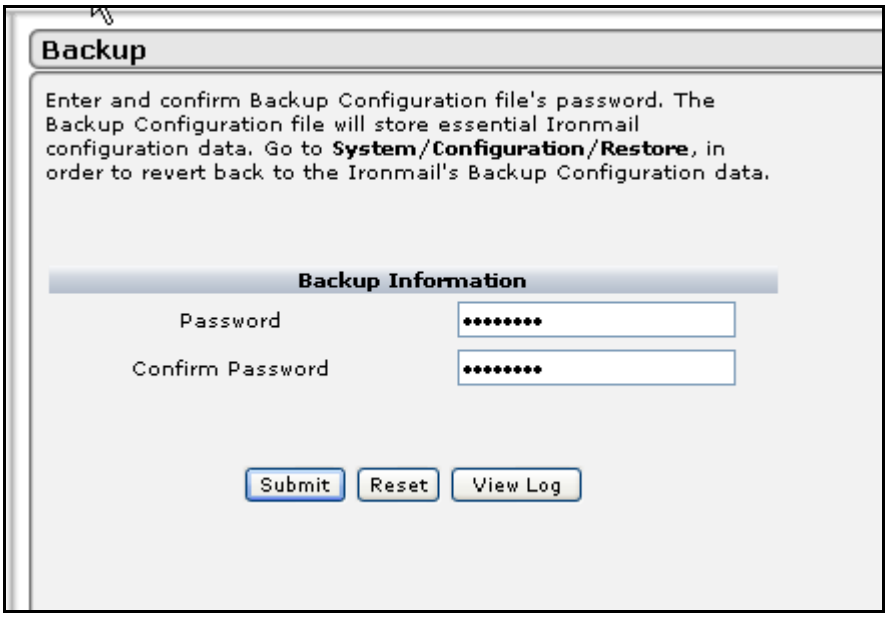
Clicking the CLI Access hyperlink opens a configuration screen where the Administrator can set the log level for command line access by selecting the desired value from the pick list and clicking **Submit**.

Clicking the CipherTrust Support Access hyperlink allows the Administrator to enter the correct port through which access is to be provided. Clicking **Submit** records the selection.

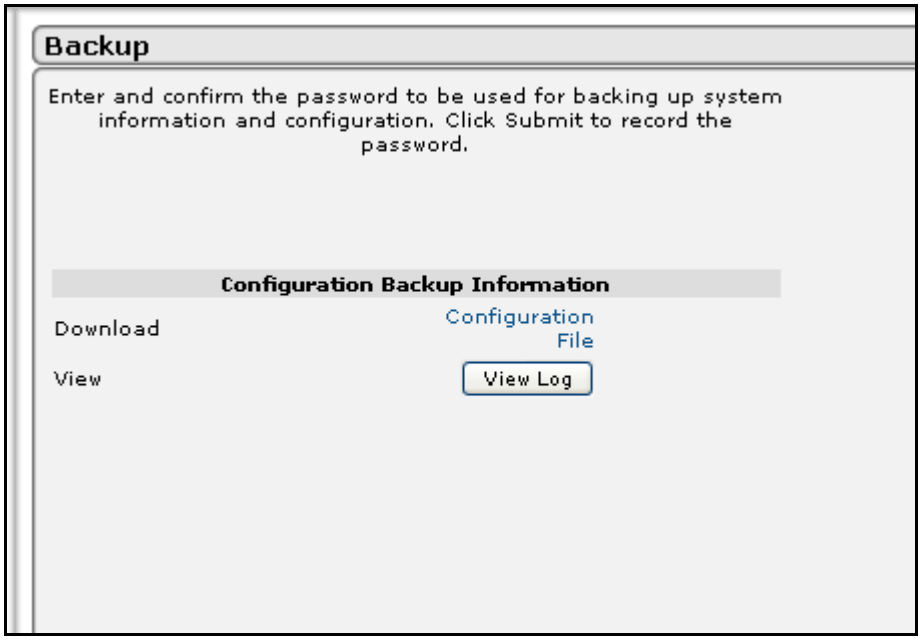


Backup

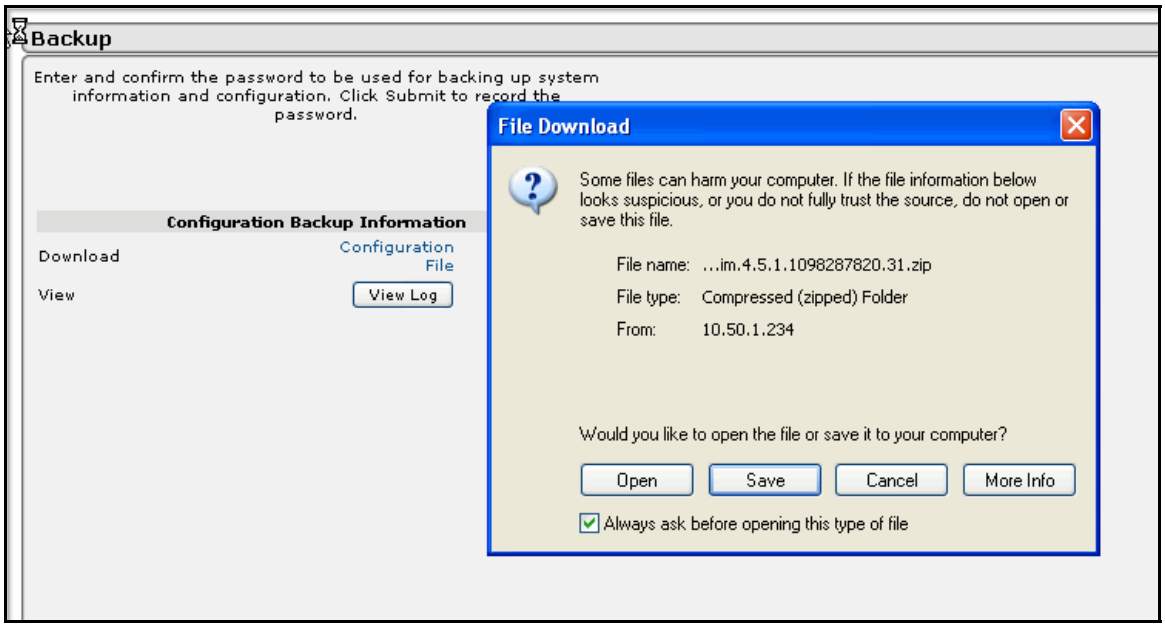
IronMail allows administrators to backup the configuration settings for the appliance (e.g., email policies, Mail and Queue Service settings, etc.) in case of disk failure. The backup should only be used to restore data to the same IronMail appliance.


Backup
Enter and confirm Backup Configuration file's password. The Backup Configuration file will store essential Ironmail configuration data. Go to System/Configuration/Restore, in order to revert back to the Ironmail's Backup Configuration data.
Backup Information
Password
Confirm Password
Submit
Reset
View Log

Enter and confirm a password to be associated with the backup file and click **Submit**. This password will be required when the backup is restored. The following screen displays.


Backup
Enter and confirm the password to be used for backing up system information and configuration. Click Submit to record the password.
Configuration Backup Information
Download
Configuration File
View
View Log

Clicking the Configuration File hyperlink will open a screen that provides information about the backup file and allows the Administrator to save the compressed folder for future use.


Backup
Enter and confirm the password to be used for backing up system information and configuration. Click Submit to record the password.
Configuration Backup Information
Download
Configuration File
View
View Log
File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: ...im.4.5.1.1098287820.31.zip
File type: Compressed (zipped) Folder
From: 10.50.1.234
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

Clicking the View Log button shows the log providing details about the execution of the backup.

```
BACKUP:10202004 11:57:00:*************************************************************************
BACKUP:10202004 11:57:00:Arguments Values Passed database <ct> opertionType <BACKUP> Push Components <>
BACKUP:10202004 11:57:00:  Backup System      Start 1098287820.31
BACKUP:10202004 11:57:00:Backing up Database
BACKUP:10202004 11:57:00:       backupDB      Start 1098287820.31
BACKUP:10202004 11:57:04:       backupDB       Stop 1098287824.7
BACKUP:10202004 11:57:04:Backing up system files.
BACKUP:10202004 11:57:04:Backup System Files      Start 1098287824.7
BACKUP:10202004 11:57:04:Backup System Files       Stop 1098287824.87
BACKUP:10202004 11:57:06:Encrypting using password.
BACKUP:10202004 11:57:06:Encoding the datafile -> /ct/w3/admin/java/webapp/webadmin/tmp/im.4.5.1.1098287820.31.zip
BACKUP:10202004 11:57:06:Cleaning the CMCTMP directory
BACKUP:10202004 11:57:06:Cleaning the CMCTMP directory done
BACKUP:10202004 11:57:06:  Backup System       Stop 1098287826.92
BACKUP:10202004 11:57:06: Completed Operation Type : <BACKUP>
```

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., im.4.5.1.1098287820.31.zip). The backup information is encrypted, stored in a proprietary file format that only IronMail can read, and cannot be viewed in Plain Text. The encryption method is "one way"—even CipherTrust Technical Support cannot decrypt this file. The "zip" file extension has been supplied to the backup file name solely for the purpose of "tricking" a browser into downloading the file, rather than trying to open it. Do not forget the password!

What Data IronMail Backs Up

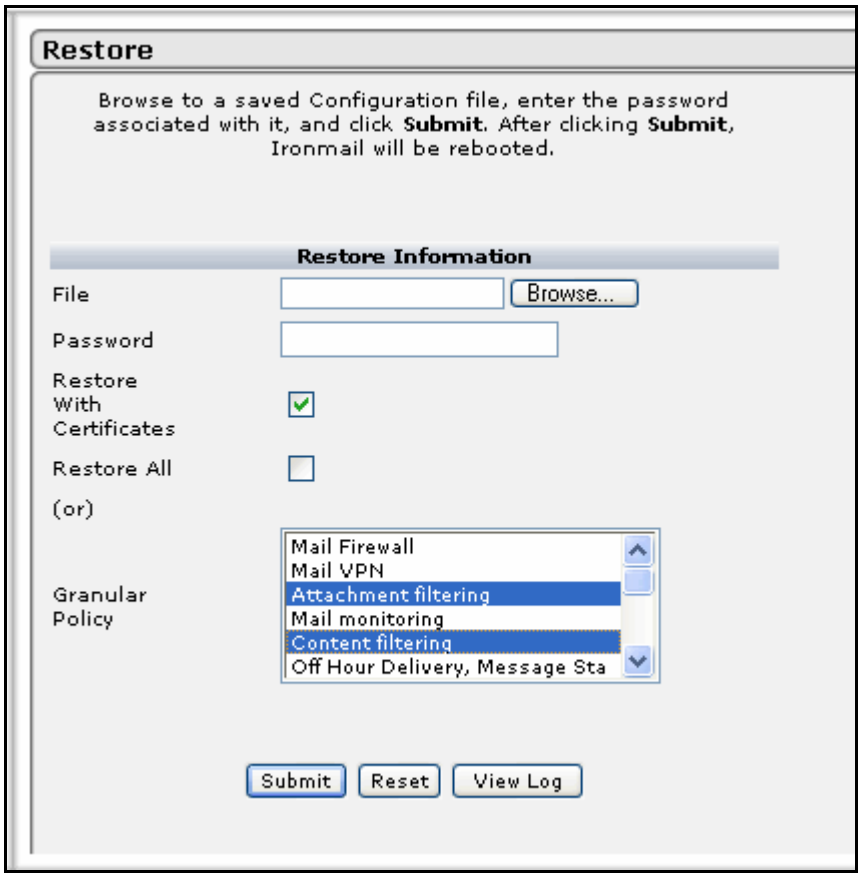
Address Masquerade configuration	Group information
Attachment Filtering *policy* configuration	Secure Delivery configuration
Alert Manager configuration	IDS Updates configuration
Anomaly Detection configuration	Security Key Management configuration
FTP/SCP archive server information, wherever configured	IronMail's mouse-over help text
ALL **User Interface** configuration not mentioned elsewhere in this table, plus secondary	LDAP configuration

configuration that the user-defined configuration controls but which is not accessible from the GUI.	
Policy Manager Bypass configuration	Mail Monitoring configuration
SMTPO bypass configuration	Name/number of IronMail patch version
Content Filtering configuration	Policy Manager configuration
Cleanup Schedule configuration	Anti-Spam configuration
Customized Notification messages	Subsystem Service configuration (Mail Services, Queue Services, etc.)
IronMail Directory Structure (internal maps of database tables)	Quarantine types
DNS Hijack configuration and information	Report configuration
Domain priority	Routing information
Information about IronMail "features"—the top-level navigation tabs in the Web Admin interface.	IDS signature configuration
Message Stamping configuration	End User Spam Reporting configuration and information
Threat Response configuration	Web Admin User Account configuration
IronMail version information	Virus configuration
Health Monitor alert list and configuration	IronWebMail configuration

Note that IronMail does *not* backup the *network* information (*IP address*, *subnet*, DNS, etc.) configured in *System > Configuration > IronMail*.

Restore

Use the Restore function to restore data only to the same IronMail appliance. Software feature licenses—e.g., for IronWebMail, Secure Web Delivery, Anti-Virus, etc.—cannot be pushed to other appliances via this "restore" method.



Field	Description
File	Enter the file name and its complete path, or browse to the backup file's location using the browse button.
Password	Enter the password associated with the backup file when it was created.
Restore with Certificates	Click the checkbox if you want to restore the security certificates that were in use by this IronMail when the backup was done.
Restore All (or) Granular Policy	If you want to restore the complete database file, click the check box. If you prefer, select the group or groups of policies to be restored.

Click **Submit** to execute the restoration. IronMail reads all the configuration data and enters it into the appliance. **The IronMail appliance will automatically reboot whenever a backup configuration is restored.**

Clicking the View Log button will open a log screen that provides details about the restoration.

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., im.4.5.1.1098287820.31.zip). The name of the IronMail is stored within the backup file that is

created. Therefore, under no circumstances rename or edit this file! Changing the file's name will cause the Restore function to fail, and may produce other unintended consequences.

Note: When an IronMail configuration is backed up, that appliance's *host name*, *IP address*/*subnet*, and User Accounts are saved. Restoring that backup configuration to another IronMail appliance will *not* over-write the second box's host name, IP address, and subnet. However, the User Accounts *will be restored*—potentially creating a security risk. If the backup file from one IronMail is restored onto another IronMail, ensure that the User Accounts are carefully reviewed and modified as required.

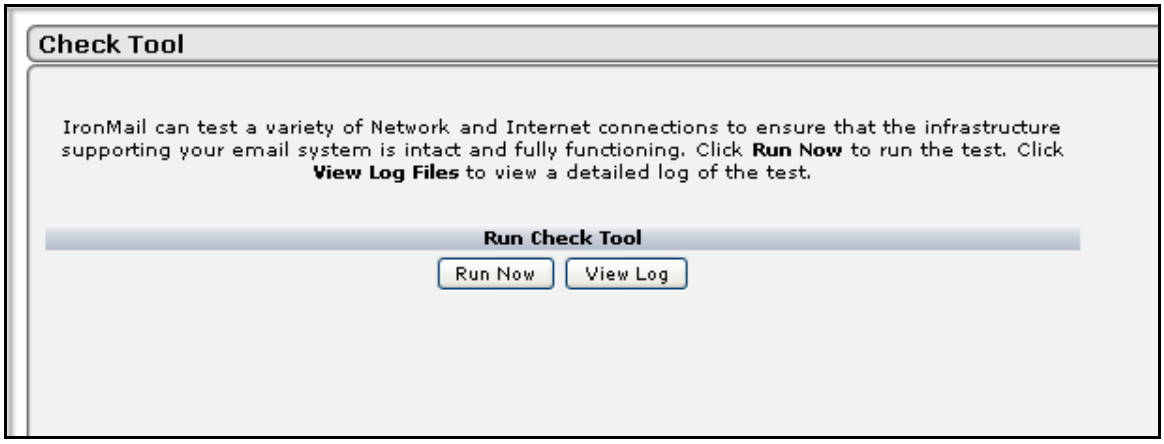
What Data IronMail Restores

Address Masquerade configuration	Group information
Attachment Filtering *policy* configuration	Secure Delivery configuration
Alert Manager configuration	IDS Updates configuration
Anomaly Detection configuration	Security Key Management configuration
FTP/SCP archive server information, wherever configured	
ALL **User Interface** configuration not mentioned elsewhere in this table, plus secondary configuration that the user-defined configuration controls but which is not accessible from the GUI.	LDAP configuration
Policy Manager Bypass configuration	Mail Monitoring configuration
SMTPO bypass configuration (Automatic whitelisting)	Web Admin User Account configuration
Content Filtering configuration	Policy Manager configuration
Cleanup Schedule configuration	Anti-Spam configuration
Customized Notification messages	Subsystem Service configuration (Mail Services, Queue Services, etc.)
End User Quarantine Release	Quarantine types
DNS Hijack configuration and information	Report configuration
Domain priority	Routing information
Anti-Virus configuration	IDS signature configuration

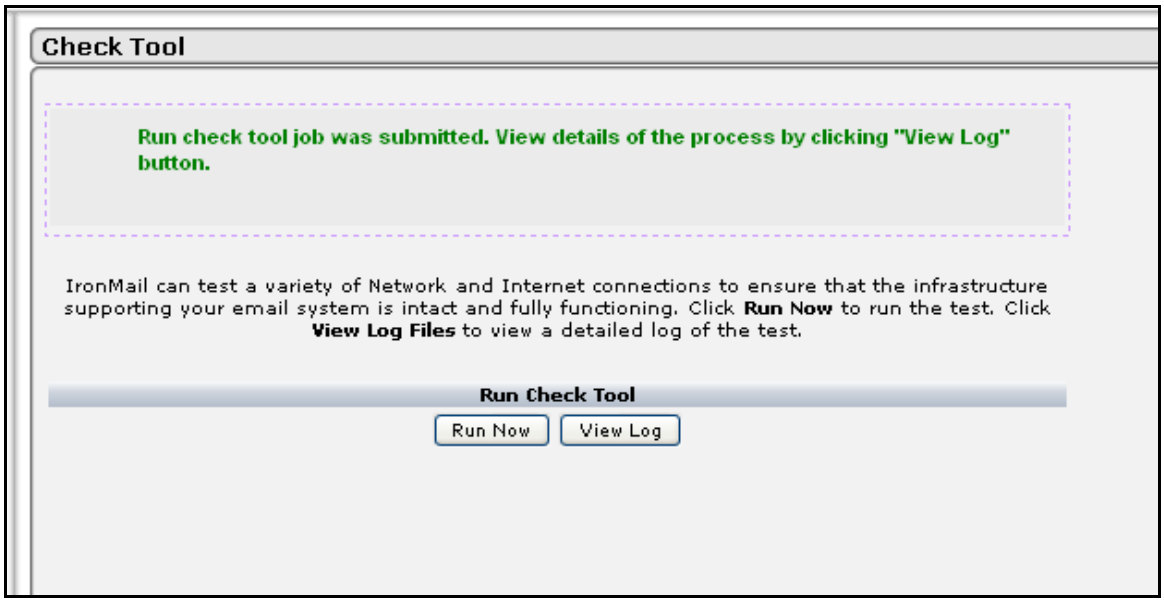
Message Stamping configuration	End User Spam Reporting configuration and information
Threat Response configuration	IronWebMail configuration
Health Monitor alert list and configuration	

Check Tool

IronMail can test a variety of *Network* and Internet connections to ensure that the infrastructure supporting the internal email system is intact and fully functioning. Specifically, it ensures that connections to internal POP, IMAP, and SMTP servers can be opened, and that the *DNS server* is reporting the correct MX and A record data. Other network connections—such as network time, alerts, SLS sync, and LDAP servers—are also tested.


Check Tool
IronMail can test a variety of Network and Internet connections to ensure that the infrastructure supporting your email system is intact and fully functioning. Click Run Now to run the test. Click View Log Files to view a detailed log of the test.
Run Check Tool
Run Now
View Log

Click **Run Now** to run the test. The screen will display a message acknowledging the job.

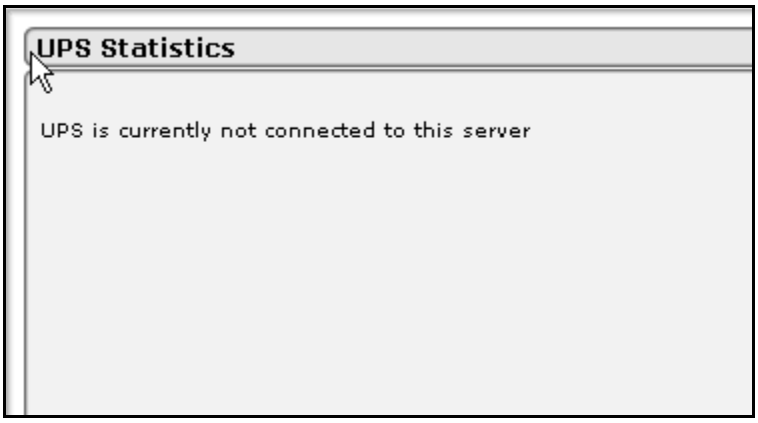

Check Tool
Run check tool job was submitted. View details of the process by clicking "View Log" button.
IronMail can test a variety of Network and Internet connections to ensure that the infrastructure supporting your email system is intact and fully functioning. Click Run Now to run the test. Click View Log Files to view a detailed log of the test.
Run Check Tool
Run Now
View Log

When the job is finished, you can click **View Log File** to view a detailed log of the results of the test. A sample of the log file is shown below.

```
Setting Name=<cmc_virtual_interface> Value = <0>
Setting Name=<ade_rule_counter> Value = <2>
Setting Name=<stm_action> Value = <108>
Setting Name=<ms_filtering> Value = <0>
Setting Name=<sendToSyslogger> Value = <0>
Setting Name=<info_log> Value = <0>
Setting Name=<product> Value = <smb>
Setting Name=<trust_rootcert> Value = </ct/conf/pubstore/trustroot.pem>
Setting Name=<encrypt_mode> Value = <1>
Setting Name=<attachedToCMC> Value = <0>
Setting Name=<allow_upward_restore> Value = <0>
Setting Name=<oob_enabled> Value = <0>
Setting Name=<route_subdomain> Value = <0>
Setting Name=<monitor_ip> Value = <localhost>
Setting Name=<shm_spamcount> Value = <100>
Setting Name=<cfReadSize> Value = <4>
Setting Name=<keyfile> Value = </ct/conf/apache/ct_serverkey.ber>
CHECKTOOL:10192004 16:00:45:Base Class readAllTables()
Summary Logger = <<rotating-file logger: <open file '/ct/data/admin/log/summary.log', mode 'a' at 0x85a3
CHECKTOOL:10192004 16:00:45:*************** BEGIN TEST ***********************
CHECKTOOL:10192004 16:00:45:              -- INTERNAL SERVERS --
CHECKTOOL:10192004 16:00:45: Protocol <IMAP4> Server <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Starting IMAP4 Connection Test with <mail.x3.ctqa.net> Server on Port <143>
CHECKTOOL:10192004 16:00:45:Connect time 0.003570
CHECKTOOL:10192004 16:00:45:SUCCESS: IMAP4 Server UP on port <143> of <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Round-Trip Time <0.004512> secs
CHECKTOOL:10192004 16:00:45: Protocol <IMAP4> Server <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Starting IMAP4 Connection Test with <mail.x3.ctqa.net> Server on Port <143>
CHECKTOOL:10192004 16:00:45:Connect time 0.001581
CHECKTOOL:10192004 16:00:45:SUCCESS: IMAP4 Server UP on port <143> of <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Round-Trip Time <0.002515> secs
CHECKTOOL:10192004 16:00:45: Protocol <POP3> Server <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Starting POP3 Connection Test with <mail.x3.ctqa.net> Server on Port <110>
CHECKTOOL:10192004 16:00:45:Connect time 0.001594
CHECKTOOL:10192004 16:00:45:SUCCESS: POP3 Server UP on port <110> of <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Round-Trip Time <0.002316> secs
CHECKTOOL:10192004 16:00:45: Protocol <POP3> Server <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Starting POP3 Connection Test with <mail.x3.ctqa.net> Server on Port <110>
CHECKTOOL:10192004 16:00:45:Connect time 0.001590
CHECKTOOL:10192004 16:00:45:SUCCESS: POP3 Server UP on port <110> of <mail.x3.ctqa.net>
CHECKTOOL:10192004 16:00:45:Round-Trip Time <0.002309> secs
```

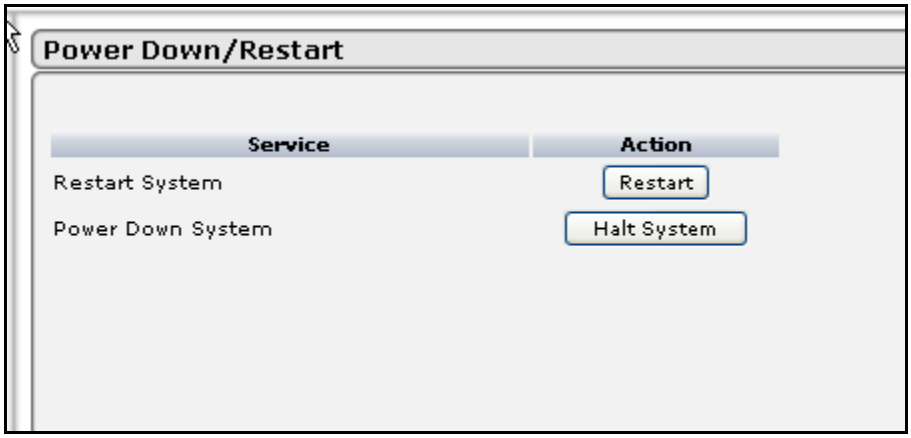
UPS Statistics

If IronMail is connected to a supported Uninterruptible Power Supply (UPS), it will display useful information about the status of the UPS (see “Uninterruptible Power Supplies” on page 239 for a table enumerating which UPS systems are compatible with IronMail). If IronMail is not connected to a supported UPS, this page will say that a UPS is not present.



Power Down and Restart

IronMail should be restarted anytime a change is made to the settings in the Configure IronMail window. Click **Restart** to restart IronMail. Note that clicking **Restart** gracefully shuts down the IronMail appliance and restarts it. This is *unlike* the **restart** command in the Command Line Interface which only restarts the Web Administration graphical user interface. Though no messages will be lost, the flow of email will be temporarily halted until IronMail has fully restarted.

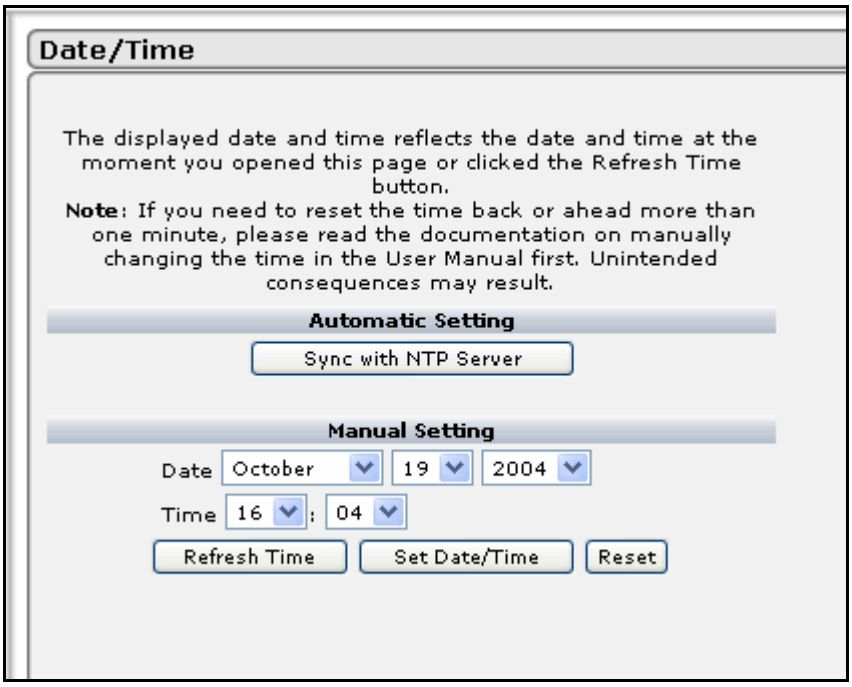


Click **Halt System** to stop all IronMail's services. It may take approximately 2 minutes for IronMail to be ready for the machine to be manually powered down. (The browser will display a message that IronMail is being powered down.) Unlike a PC, shutting down IronMail stops all of its services without powering down the hardware. To completely turn off IronMail, press and hold down the on/off button on the front of the appliance for 4 seconds.

After IronMail is running, ***never*** press the reset switch on the front of the appliance until IronMail has been gracefully shut down from within either the graphical Web Administration or Command Line interface. Pressing the reset switch while IronMail is currently running forces IronMail to "hard boot"—a process that will corrupt its internal databases, and render it inoperable. Damage to IronMail's database will require CipherTrust's Technical Support engineers to manually repair and rebuild the corrupted files.

Date and Time

The displayed date and time reflects IronMail's internal date and time at the moment this page is opened or the **Refresh Time** button is clicked. If NTP time servers are entered in *System > Configuration > IronMail* window, IronMail "syncs" itself with one of the servers once every minute.


Date/Time
The displayed date and time reflects the date and time at the moment you opened this page or clicked the Refresh Time button.
Note: If you need to reset the time back or ahead more than one minute, please read the documentation on manually changing the time in the User Manual first. Unintended consequences may result.
Automatic Setting
Sync with NTP Server
Manual Setting
Date October 19 2004
Time 16 : 04
Refresh Time
Set Date/Time
Reset

Manually adjust the time or date by specifying date and time values from the pick lists. After manually entering new values, click **Set Date/Time** to update IronMail.

If a time or date is entered *further ahead than the administrative inactivity time-out interval* (*System > Web Admin > Configure > "Administrative Time-out"*), IronMail will log out all administrators currently logged onto the graphical user interface. Simply log back in and continue the administrative session as usual.

If the time is reset backward, administrators will be prompted to reboot the appliance in order for the setting to take effect.

Extreme caution should be used whenever manually changing the internal IronMail time and date more than one minute from what the NTP time server is reporting. (If NTP server information was provided in IronMail's Configuration window, IronMail automatically synchronizes with the server once every minute.) Within the next minute after the time is manually changed, the automatic time server synchronization will reset IronMail's clock again.

Manually changing the internal clock more than one minute ahead or back ***will also affect IronMail's queues*** (e.g., Outbound Queue, Content Filtering Queue, etc.) and mail services (e.g., SMTPI Service, SMTPO Service, etc.). These processes all run on a "cycle time"—on average, several times a minute. After processing messages and before "going to sleep," they calculate the time stamp for when they will next "wake up" to process new messages. If the internal clock is moved forward one whole day, for example, the queues and services will instruct IronMail that their next "wake up" time is going to be tomorrow plus *nnn* seconds (where *nnn* = the real cycle time). However, one minute later, the time servers will re-sync IronMail's clock back to *today* without resetting IronMail's queues' and mail services' "wake up" time. The queues and services will wait until tomorrow to wake up and begin processing messages again. **Therefore, if the clock is ever manually changed by more than one minute, always stop and restart each of the queues and services to reset their "wake up" times.**

Force IronMail to immediately synchronize with an Internet Time (NTP) Server by clicking **Sync with *NTP Server***. Note that the name of a valid time server must have entered in the *System > Configuration > IronMail* page to do this.

Note that IronMail writes a timestamp in its database noting when each message enters the Outbound Queue for delivery. IronMail uses this timestamp as a reference for when it may "pick up" messages for delivery. Therefore, if the clock is set backward and there are currently messages in the outbound queue, those messages' delivery will be delayed until IronMail's internal clock "catches up" to the time-stamp originally entered in the database.

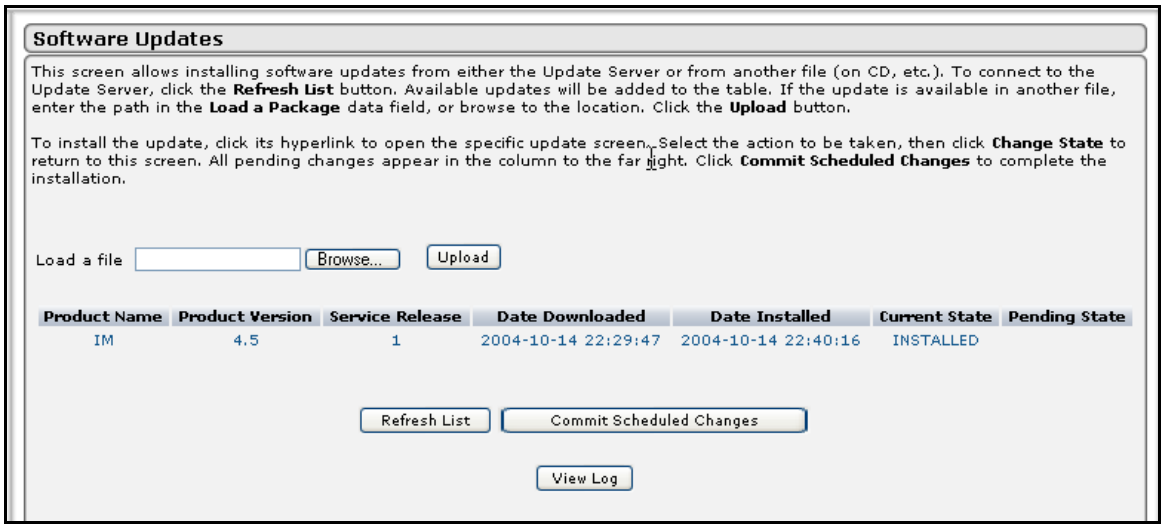
Daylight Savings Time

IronMail automatically adjusts for Daylight Savings Time (DST) at 2 A.M. on the first Sunday of April and reverts to Standard Time at 2 A.M. on the last Sunday of October.

System Updates

Software Updates

The Software Update Management table, empty until the CipherTrust Update Server has been queried, displays information about installed software and file updates available for installation. The table displays the following information:

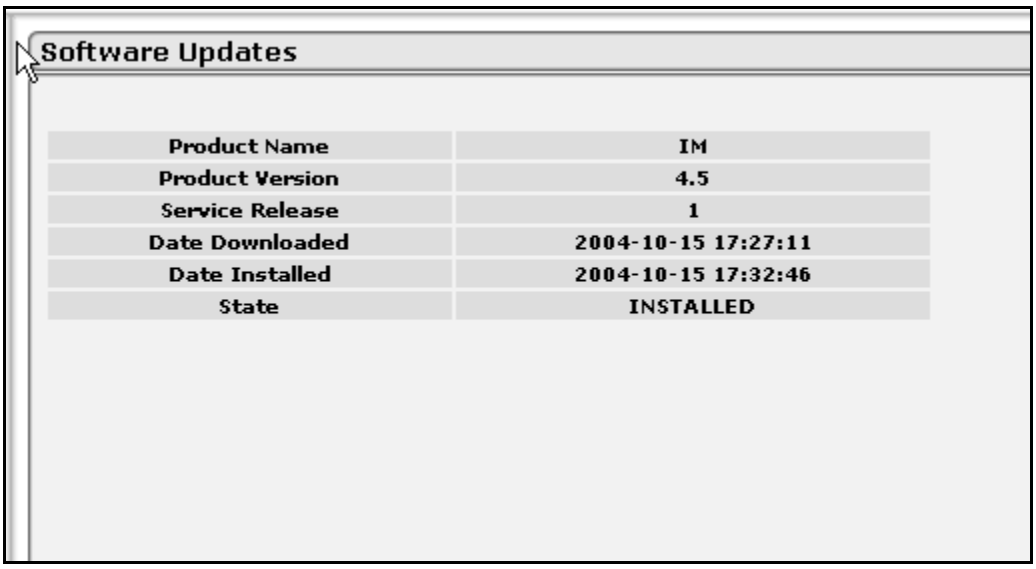

Software Updates
This screen allows installing software updates from either the Update Server or from another file (on CD, etc.). To connect to the Update Server, click the Refresh List button. Available updates will be added to the table. If the update is available in another file, enter the path in the Load a Package data field, or browse to the location. Click the Upload button.
To install the update, click its hyperlink to open the specific update screen. Select the action to be taken, then click Change State to return to this screen. All pending changes appear in the column to the far right. Click Commit Scheduled Changes to complete the installation.
Load a file
Browse...
Upload
Product Name
Product Version
Service Release
Date Downloaded
Date Installed
Current State
Pending State
IM
4.5
1
2004-10-14 22:29:47
2004-10-14 22:40:16
INSTALLED
Refresh List
Commit Scheduled Changes
View Log

Product Name	This column displays the name of the CipherTrust product (e.g., IronMail or *Centralized Management Console*).
Product Version	This column displays the version number of the software. (The version of software this document describes is version 3.1.)
Service Release	This column displays the name of the Service Release. (Service Releases are named in incremental numbers in ascending order.)
Date Downloaded	This column displays the date when the software file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the software file was installed on the appliance.
Current State	This column displays the software file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed.

	• **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

The **Refresh List** button sends a request directly to CipherTrust's update server, which will populate your IronMail Software Updates page with its list of available file updates.

Any value in each row of the table of software files is a hyperlink that opens a details screen.

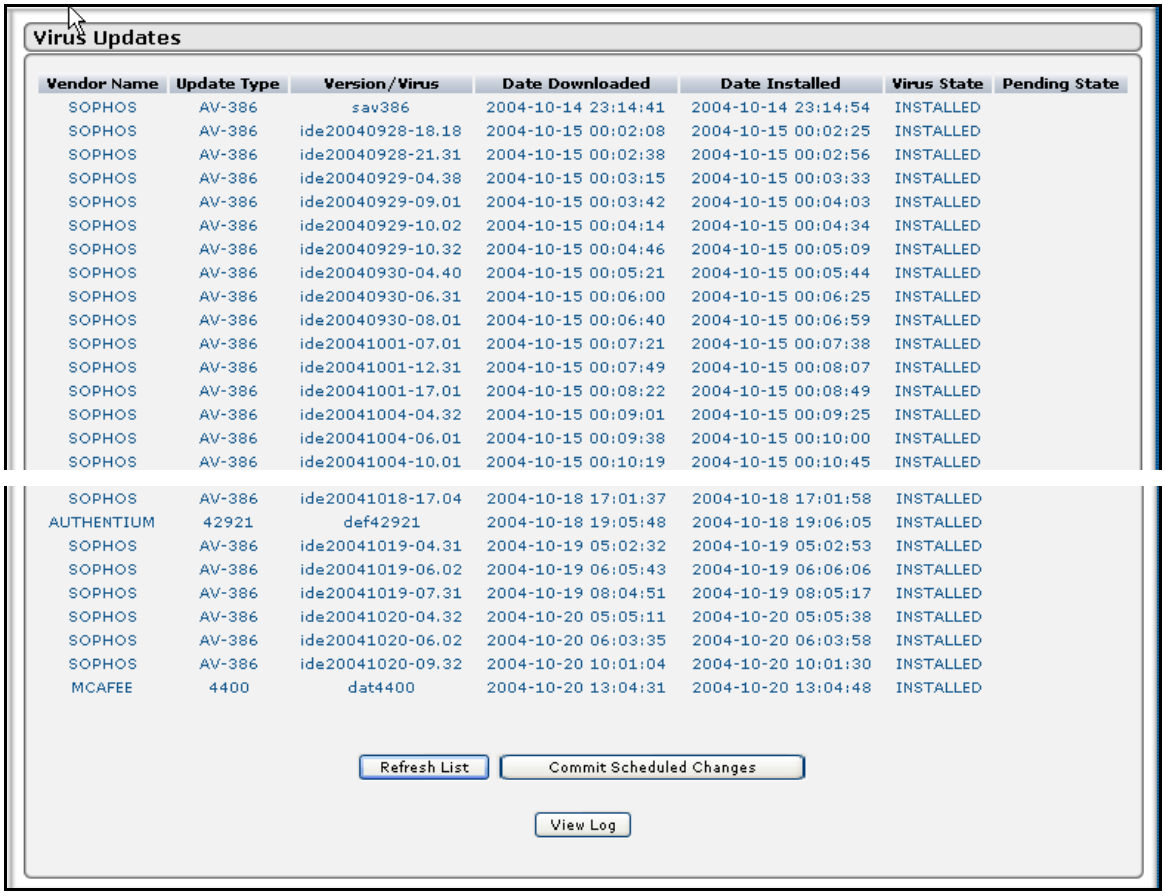


The details of the file are shown again, and if the update is either Available or Downloaded,a **Change State** pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Software Update Management table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Clicking the **View Log File** button opens a new browser window showing the status of the update process.

Virus Updates

The Virus Update Management table, empty until the CipherTrust Update Server has been queried, displays information about installed software and file updates available for installation.



The table displays the following information:

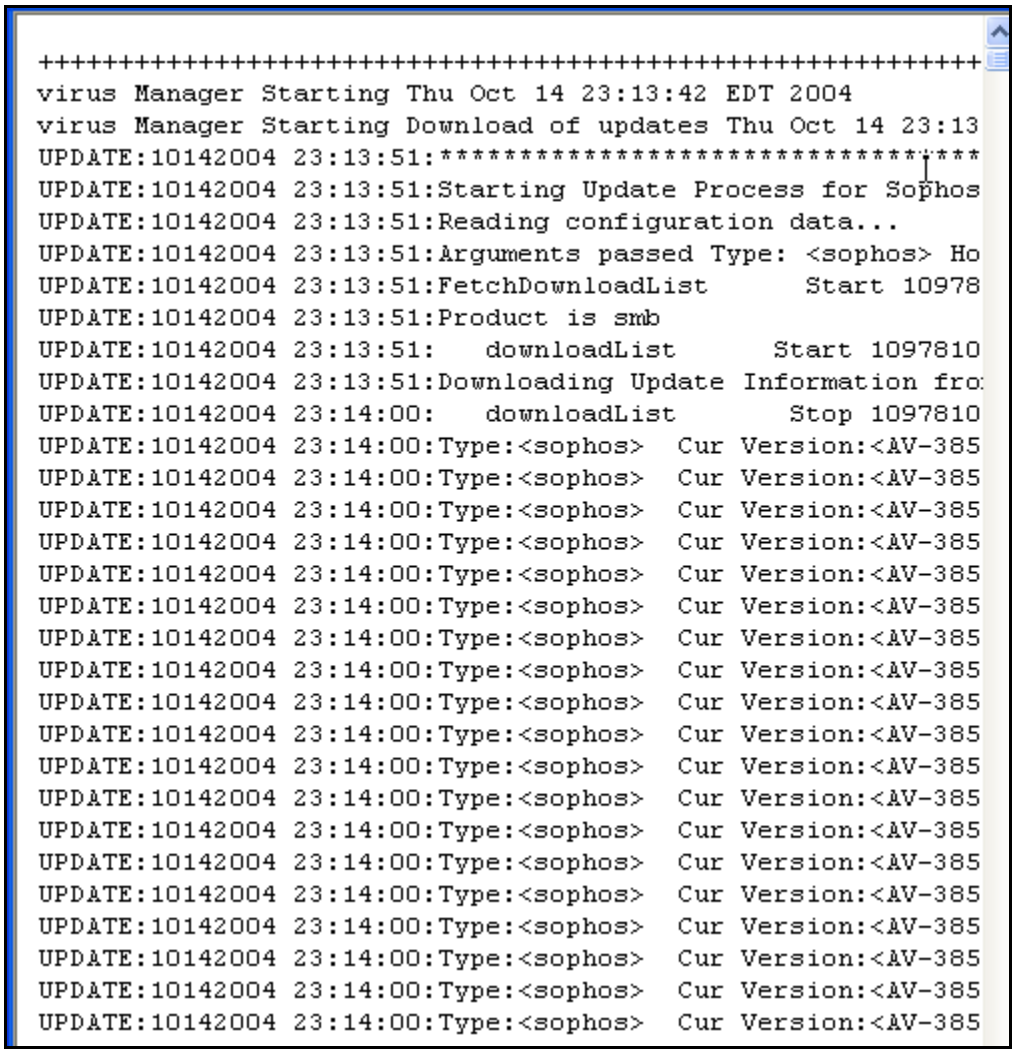
Vendor Name	This column displays the name of the anti-virus vendor (e.g., Sophos or McAfee).
Update Type	This column displays whether the file is an “engine” (the latest anti-virus engine that “rolls up” the latest virus definitions) or an individual virus identity file (created since the latest engine was released).
Version/Virus	This column displays the name virus engine or specific identity file.
Date Downloaded	This column displays the date when the anti-virus file was downloaded to IronMail’s disk.
Date Installed	This column displays the date when the anti-virus file was installed on the appliance.
Virus State	This column displays the anti-virus file’s current state. The “state” can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust’s Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed.

	• **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

The **Refresh List** button sends a request directly to CipherTrust's update server, which will populate your IronMail Anti-Virus Updates page with its list of available file updates.

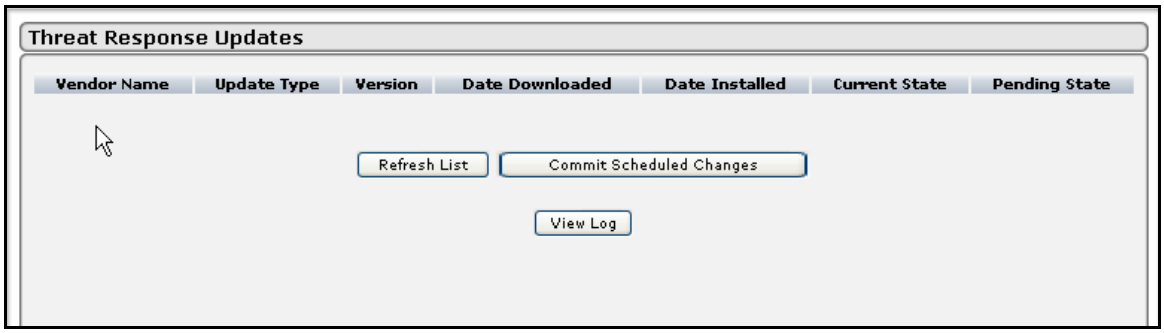
Any value in each row of the table of software files is a hyperlink that opens a "Change State" page in the main content page of the Web Administration interface. The details of the file are shown again, and a **Change State** pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Anti-Virus Update Management table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Clicking the **View Log File** button opens a new browser window showing the status of the update process.



Threat Response Updates

The Threat Response Update Management table, empty until the CipherTrust Update Server has been queried, displays information about installed threat response updates available for installation.



The table displays the following information:

Vendor Name	This column displays the name of the CipherTrust product (e.g., Threat Response).
Update Type	This column displays an update type of CT.
Version	This column displays the version identifier for the software.
Date Downloaded	This column displays the date when the Threat Response file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the Threat Response file was installed on the appliance.
Current State	This column displays the Threat Response file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

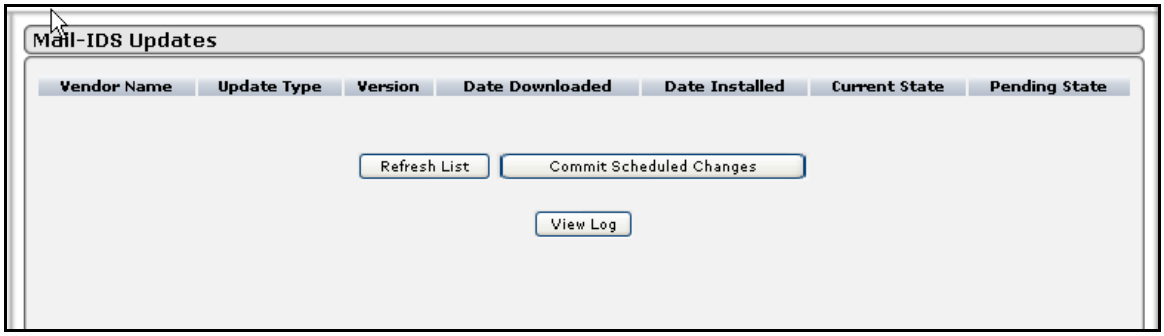
The **Refresh List** button sends a request directly to CipherTrust's Update Server, which will populate your IronMail Threat Response Update Management page with its list of available file updates.

Any value in each row of the table of Threat Response files is a hyperlink that opens a "Change State" page in the main content page of the Web Administration interface. The details of the file are shown again, and a **Change State** pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Threat Response Update Management table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Clicking the **View Log** button opens a new browser window showing the status of the update process.

Mail-IDS Updates

The Mail-IDS Update Management table, empty until the CipherTrust Update Server has been queried, displays information about installed software and file updates available for installation.



The table displays the following information:

Vendor Name	This column display the name of the vendor of the software update. CT is displayed.
Update Type	This column displays an Update Type of IDS.
Version	This column displays the version number of the IDS engine or specific identity file.
Date Downloaded	This column displays the date when the Mail-IDS file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the Mail-IDS file was installed on the appliance.
Current State	This column displays the Mail-IDS file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed. • **Uninstalled:** Software files may not be uninstalled—this option has been added to the user interface for future functionality.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

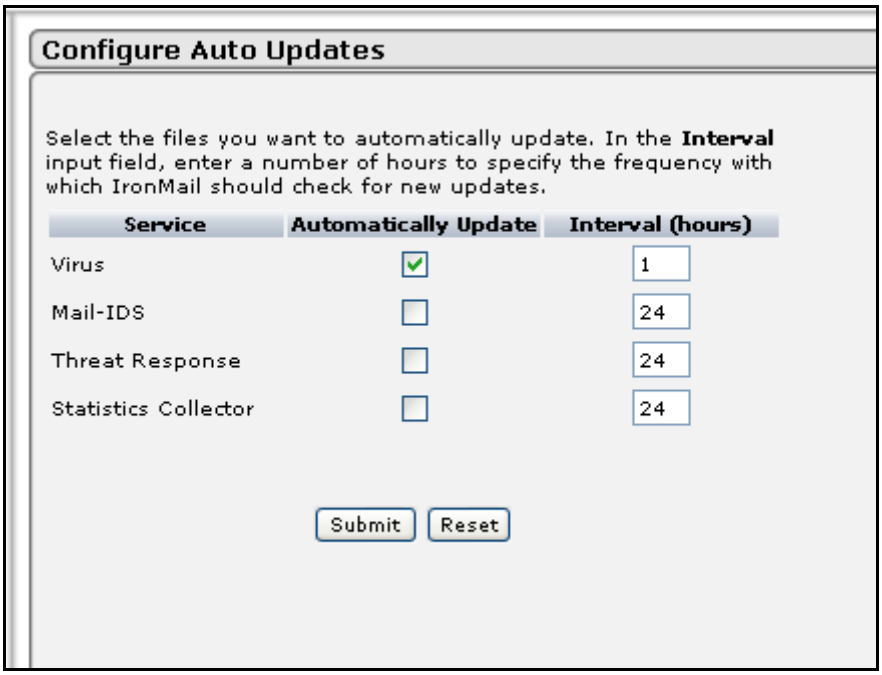
The **Refresh List** button sends a request directly to CipherTrust's Update Server, which will populate your IronMail Mail-IDS Update Management page with its list of available file updates.

Any value in each row of the table of Mail-IDS files is a hyperlink that opens a "Change State" page in the main content page of the Web Administration interface. The details of the file are shown again, and a "Change State" pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Mail-IDS Update Management table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Clicking the **View Log File** button opens a new browser window showing the status of the update process.

Configure Auto-Updates

The Configure Auto Updates sub-menu displays the licensed Subscription Services installed on the appliance. Each Service may be configured to query CipherTrust's update server for newly available files. IronMail will automatically download and install any files that become available.



Select the check box for **Automatically Update** to enable auto-updating for a licensed feature. When enabled, IronMail will query the update server on the specified interval for newly available files. Files are installed unattended in the background. Enter a number of hours (from 1-24) in the **Interval** input field indicating how often the IronMail should query CipherTrust's update server for newly available files.

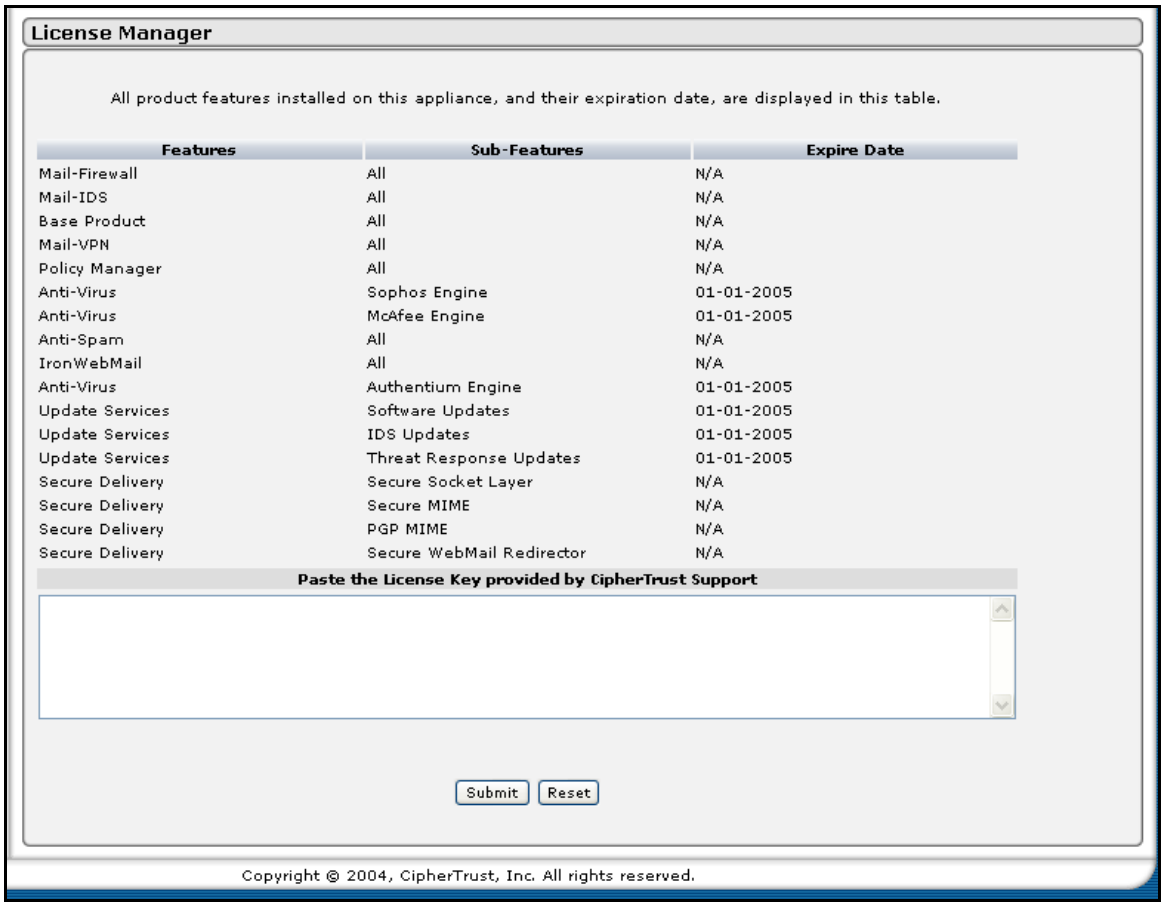
Column	Explanation
Service	This column lists the services for which automatic updates are available. You may choose any or all of the following: • Virus - automatic updates to the licensed anti-virus engines configured for your IronMail appliance; • Mail_IDS - automatic updates to CipherTrust's Intrusion Detection System; • Threat Response - automatic updates providing the latest "best practice" configurations, including responses to new threats; and, • Statistics Collector - automatically downloads data collection scripts to aid issue analysis and research efforts. The collected data may be securely copied (using SCP) back to the CipherTrust Research Group. In order to enable Statistics Collector updates, you must also enable Global Settings as part of Configuring Queues (in Queue Manager). You may enable either or both the following global settings:

	• Enable Statistical Information to be shared with CipherTrust Research, and • Allow Spam and Other Message Information to be shared with CipherTrust Research.
Automatically Update	Checking the check box for any service enables the automatic updates for that service. Leaving the boxes unchecked disables the individual services.
Interval (hours)	Entering a number in this data field sets the interval between queries for new updates. The intervals are set in numbers of hours.

Click **Submit** to save the input.

License Manager

The License Manager table shows all Product Licenses that have been installed on IronMail. Some of the Licenses correspond to the "tabbed" program areas in the IronMail interface (e.g., Mail-Firewall, Mail-VPN, etc.), where others refer to subscription services (e.g., Anti-Virus, Threat Response Updates, etc.).


License Manager
All product features installed on this appliance, and their expiration date, are displayed in this table.
Features
Sub-Features
Expire Date
Mail-Firewall All N/A
Mail-IDS All N/A
Base Product All N/A
Mail-VPN All N/A
Policy Manager All N/A
Anti-Virus Sophos Engine 01-01-2005
Anti-Virus McAfee Engine 01-01-2005
Anti-Spam All N/A
IronWebMail All N/A
Anti-Virus Authentium Engine 01-01-2005
Update Services Software Updates 01-01-2005
Update Services IDS Updates 01-01-2005
Update Services Threat Response Updates 01-01-2005
Secure Delivery Secure Socket Layer N/A
Secure Delivery Secure MIME N/A
Secure Delivery PGP MIME N/A
Secure Delivery Secure WebMail Redirector N/A
Paste the License Key provided by CipherTrust Support
Submit
Reset
Copyright © 2004, CipherTrust, Inc. All rights reserved.

Each License's expiration date is also displayed.

The following Licenses are available for IronMail:

- **Mail-Firewall** (providing configuration and encryption for message sending)
- **Mail-IDS** (providing 24/7 protection against *network* attacks)

- **Base Product** (offering the base functionality of IronMail's hardened face and ability to proxy email)
- **Mail-VPN** (providing configuration and encryption for message retrieval)
- ***Policy*** **Manager** (allowing the creation and enforcement of email policies)
- **Authentium Anti-Virus** (providing virus protection)
- **Sophos Anti-Virus** (providing virus protection)
- **McAfee Anti-Virus** (providing virus protection)
- **Anti-Spam** (providing anti-spam protection)
- **Secure Delivery** (providing a variety of options to ensure that a message is delivered securely—e.g., *SSL*, S/*MIME*, PGP or HTTPS)
- **IronWebMail** (allowing proxying and protection for your web mail system)
- **Maintenance** (providing 24/7 Technical Support and IronMail software updates)
- **Threat Response Updates** (providing timely "policies" designed to protect against email threats for which no other solution currently exists)
- **Signature Updates** (providing timely updates to the Mail-IDS signatures used to detect hacker attacks)

Administrators can add licenses or extend the expiration date for product features or services at any time. (Licenses accumulate—that is, concatenate—on the appliance.)

Note: If a Secure Delivery license is installed *after* IronMail's initial installation, the administrator must logout and log back in to IronMail's Web Administration in order for the Secure Delivery program tab to display in the top navigation bar of the Web Admin interface. Also, when an anti-virus licenses expires, it disappears from the Web Administration interface and its functionality ceases on the midnight *before* the date of expiration. Anti-virus license renewals should be installed *prior* to license expiration. If a renewal license is installed *after* license expiration, administrators will have to manually re-configure anti-virus settings and place the Virus Scan Queue back into the Queue Order.

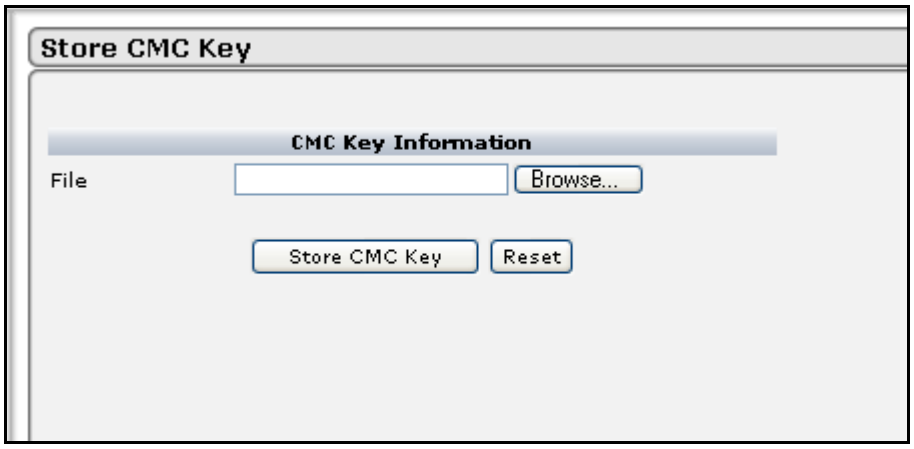
In enterprise environments where Centralized Management Consoles (*CMC*) are managing multiple IronMail "slaves," the CMC is responsible for acquiring and renewing all licenses. The CMC will automatically push product feature or service licenses to its IronMails.

While administrators were prompted to install a License Key when first running the IronMail Initial Configuration Wizard, they may install additional Licenses within this License Manager window. Paste in the License Number input field the "key" that CipherTrust Technical Support issued and click **Submit**. That program area that key enables is immediately available after logging out of the Web Administration interface and logging back in.

Store CMC Key

The Centralized Management page allows administrators to configure an IronMail appliance as a "slave" to another IronMail configured as a Centralized Management Console (*CMC*) "master." In enterprise environments with multiple IronMails protecting multiple domains and mail servers, centralized management allows an administrator to easily manage policies, push software and anti-virus file updates, as well as pull logs, reports, and alert messages.

Contact CipherTrust Sales to learn if *Centralized Management Console* architecture can aid in a particular enterprise email environment.



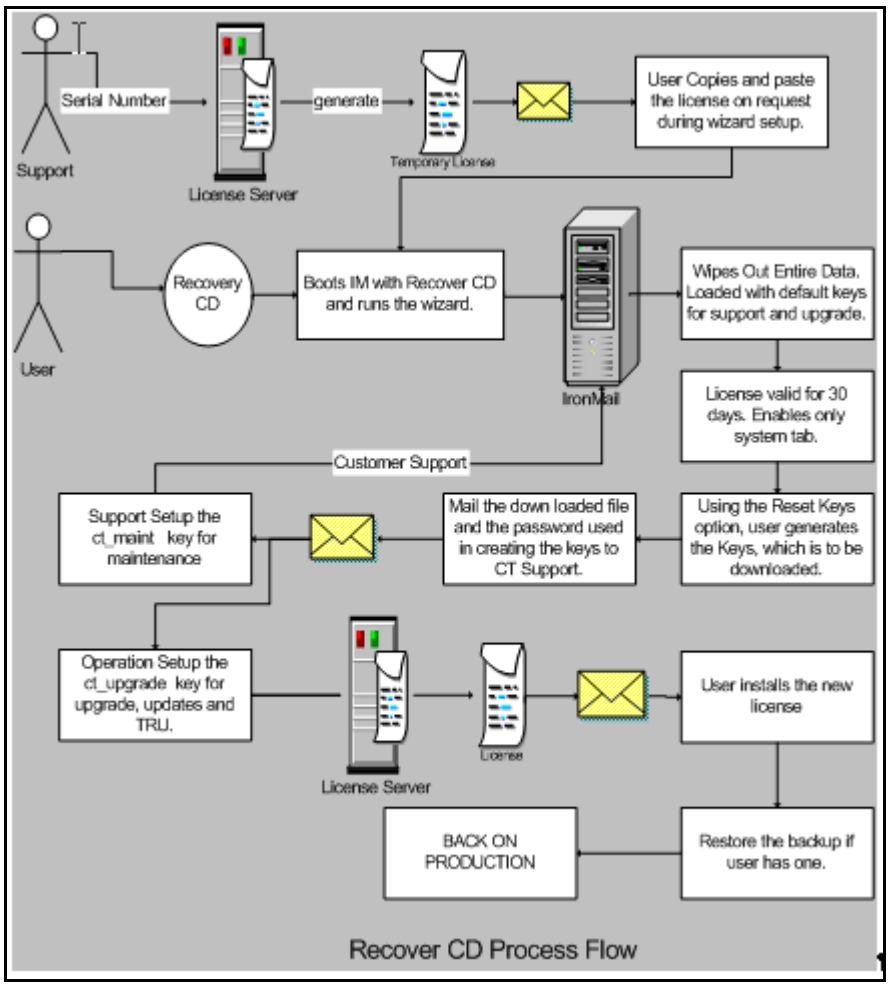
The Store CMC Key page contains a **Browse** button. Use it to navigate to the file containing the Centralized Management Console's (CMC) "public key" which the CMC Administrator exported and saved to disk. The master/slave connections can only be mediated though this public key. The key provides for encrypted sessions between the CMC and its slaves—a master and slave cannot communicate without it.

After navigating to and selecting the CMC's public key file, click **Store CMC Key** to install the CMC's public key.

The **Reset** button clears the **Browse** navigation input field if Store CMC Key has not yet been clicked.

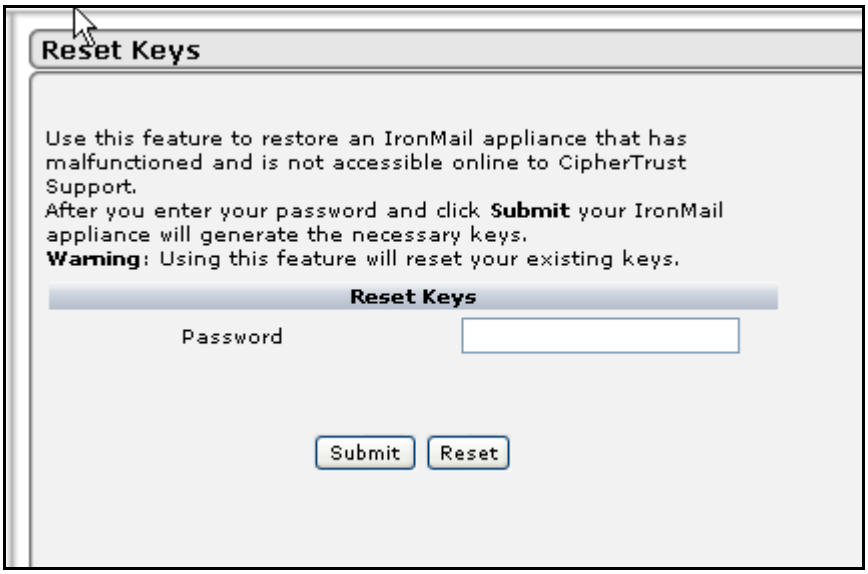
Resetting Keys

If an IronMail appliance breaks down due to unexpected events, and is not accessible online to CipherTrust Support, the appliance may be restored using a Recovery CD. The process for this restoration is shown in the following flow diagram.


Support
Serial Number
License Server
generate
Temporary License
User Copies and paste the license on request during wizard setup.
User
Recovery CD
Boots IM with Recover CD and runs the wizard.
IronMail
Wipes Out Entire Data. Loaded with default keys for support and upgrade.
License valid for 30 days. Enables only system tab.
Customer Support
Support Setup the ct_maint key for maintenance
Mail the down loaded file and the password used in creating the keys to CT Support.
Using the Reset Keys option, user generates the Keys, which is to be downloaded.
Operation Setup the ct_upgrade key for upgrade, updates and TRU.
License Server
License
User installs the new license
BACK ON PRODUCTION
Restore the backup if user has one.
Recover CD Process Flow

The following steps are required for restoring the IronMail appliance:

1. CipherTrust Support ships a Recovery CD to the customer.
2. The Administrator boots the IronMail appliance using the CD. The CD installs the fresh CTBSD (the customized operating system) on the IronMail, and the user is asked for the serial number of the IronMail appliance.
3. Support also mails the customer a temporary license, valid for 30 days. This license only enables the System tab in the IronMail interface. The license is generated using the default ct_maint key.
4. The Administrator runs the setup wizard. The license is required at this stage of the process.


Reset Keys
Use this feature to restore an IronMail appliance that has malfunctioned and is not accessible online to CipherTrust Support.
After you enter your password and click Submit your IronMail appliance will generate the necessary keys.
Warning: Using this feature will reset your existing keys.
Reset Keys
Password
Submit
Reset

5. The Administrator uses the screen shown above (System > Reset Keys) and the instructions that follow to create new keys for ct_maint, ct_upgrade and *cmc*. **Note:** This action will overwrite all default keys.
6. The Administrator downloads the encrypted file <serialnum>-keys.zip. The Administrator sends the downloaded file and the password used in creating the keys to CipherTrust Support.
7. Support places the new keys in operation by:
    - deciphering the setup file and replacing the old keys with the new ones
    - generating the new license using the new keys
    - emailing the new (permanent) license to the customer
8. The customer installs the new license, which enables all licensed features of IronMail, and, if a backup exists, restores the backup on the IronMail.

The Command Line

Command Line Interface

IronMail allows the Administrator to access much of the functionality available through the Graphical User Interface (GUI) from the command line. The Administrator may access the command line through either of two methods:

- via the Console, which is a keyboard connected directly to the IronMail appliance, or
- from a workstation, using a Secure Shell (SSH).

Role management for the command line is accomplished at log-in. The user name and password the Administrator enters will be used to verify access rights and permissions.

From the Console:

If a keyboard and a monitor are connected to the IronMail appliance and the IronMail is currently running, the monitor shows a log-on prompt. The keyboard must be attached to the IronMail appliance before the appliance is powered on. After the Administrator enters a valid user name and password, the command functions may be accessed by typing simple commands.

The user name and password should generally be the same as those used for GUI access. It is important to remember that, unlike using GUI functions, the Administrator will NOT be logged off after a pre-configured period of time; the log-in remains active until the Administrator logs out. For security reasons, one should not walk away from the console without first logging out by typing ***exit*** at the command prompt.

From a Secure Shell:

The Administrator may also access the command line from a workstation that uses a Secure Shell application (via port 22). The Administrator logs in by entering a valid GUI user name and password.

If the appliance is an IronMail 210 or 345 model, each of which contains two *Network* Interface Cards (NICs), and if Out-of-Band Management is enabled, the hostname of the Out-of-Band NIC will be required to allow connection to the CLI. The IronMail 305 also has two NICs, but it does not support Out-of-Band Management.

SSH clients vary widely, and keyboard mapping is different from client to client. Depending upon which client you are using, you may be required to re-map the ***backspace*** key.

Once logged in, the Administrator is able to enter commands as necessary.

The Commands

Command Overview

Commands consist of a *command word* followed by one or more *parameters*. Separate the command word and the parameters from each other with a single space. Press Enter after the last parameter to execute the command. The information that appears in the CLI complies with any restrictions or parameters that have been configured in the GUI. Any restrictions or permissions applicable in the GUI also apply to the CLI. Furthermore, the amount of information in the IronMail's detailed logs viewed in the GUI is controlled by the logging level set in the IronMail GUI.

CipherTrust does not provide customers root access to the appliance; therefore, the CLI has limited shell capabilities. Many of the commands found in a UNIX environment are not available. Only the following commands may be executed:

help, edit, run, set, show, system, tail, and test.

The table below provides more information

Command	First-level parameter	Equivalent GUI Role	Access
help	edit, run, set, show, system, tail, test (plus additional parameters)		Typing **help** at the prompt displays commands and associated text. Typing **help** before any command word or command string displays help for that subset of the command line.
edit	interface route support	System System System	Read, Write Read, Write Read, Write
run	clean quarantine clean message reports	Queue Manager Queue Manager Reporting	Read, Write Read, Write Read Only
set	serial enable service disable service stop service start service user unlock	System System System System System System	Read, Write Read, Write Read, Write Read, Write Read, Write Read, Write
show	log mapping *network* queue services system	Reporting Reporting System Reporting Reporting System	Read Only Read Only Read Only Read Only Read Only Read Only
system	reboot restart restore shutdown	System System System System	Read, Write Read, Write Read, Write Read, Write
tail	log	Reporting	Read Only
test	dns mail ping port route server	System System System System System System	Read Only Read Only Read Only Read Only Read Only Read Only

The HELP Command

On-screen help may be accessed by typing **help**. If one types **help** at the IronMail command prompt, the screen will display the top-level commands that may be used (along with any associated help text). Typing **help** before any allowed command word (**edit**, **run**, **set**, **show**, **system**, **tail** or **test**) or command string (command word plus parameters) displays help for that subset of the CLI.

```
ironmail: help

Command Summary

The words appearing on the line below are the top level commands. Type an individual word to see
the parameters for that command.  Type 'help <word>' to see help for that command.
  help     edit     run     set     show     system     tail     test

Commands are composed of a command word followed by one or more parameters.  Separate the
command word and parameters from each other with a single space.  Press Enter after the last
parameter.
On-screen help is available by typing 'help'. Typing 'help' before any command word displays help
for that command.  For some commands, typing 'help' before the command word and parameters
can provide more information.
ironmail:
```

The simulated screen shot below displays the allowable parameters and help text for the **help edit** command.

```
ironmail: help edit

The EDIT command is used to edit network interface, routing table as well as enable or disable the
support access feature.
Command Summary:
edit    interface       primary
                        oob
        route           add
                        delete
        support         enable
                        disable
```

The EDIT Command

The **edit** command is used to modify specific configuration settings for the parameters **interface**, **route** and **support**. It impacts the way IronMail appears to and works with clients.

Examples showing the syntax for the edit command are shown in the simulated screen shot below.

```
Command Summary:

edit    interface       primary
                        oob
                        clearpending
        route           add
                        delete
```

```
        support     enable
                    disable

ironmail: edit interface primary
<PRIMARY> IP Address [10.50.1.234]
<PRIMARY> Netmask [255.255.255.0]
<PRIMARY> Select media type from the list, or press ENTER to use default:
          0. Default
          1. autoselect
          2. 10baseT/UTP
          3. 10baseT/UTP (full-duplex)
          4. 100baseTX
          5. 100baseTX (full-duplex)
          6. 1000baseTX
          7. 1000baseTX (full-duplex)
          Media Type (0-7) [0]:
Warning! The setting will affect the way IronMail works with clients. Are you sure (Y/N) n
Change has been discarded.
```

The RUN Command

The **run** command allows the Administrator to execute specific commands at will. The two commands permitted are **run clean** (to clean *expired or deleted messages* in a quarantine queue, to clean *expired messages* in other queues) and **run reports** for a specified date. These commands may be configured within the GUI to execute on a daily basis without intervention, but the **run** command allows on-command execution.

Because it executes a complex SQL query of the IM database, the **run** command, whether for cleaning or reporting functions, will have a significant impact on overall performance. Therefore, this command should always be scheduled to run at a non-peak utilization period.

The simulated screen below shows the parameters and syntax for the **run clean** command string. The **run clean quarantine** command will clear or delete messages in the quarantine queue that have reached the time limit specified when the queues are configured. The **run clean message** command will clear or clean messages in other queues that have met the configured time limit.

```
Command Summary:

run     clean     quarantine
                  message
        reports   <MM/DD/YYYY>

ironmail: run clean quarantine
Forcing immediate clean-up will highly impact the performance of the appliance. Are you sure?
(Y/N) n
Discarded the changes.
ironmail:
```

```
ironmail: run clean message
Forcing immediate clean-up will highly impact the performance of the appliance. Are you sure? (Y/N)
Discarded the changes.
ironmail:
```

The parameters and syntax for the **run report** command are as shown below. The run report command will create all enabled reports from the Reports Configuration screen, with the exception of the Policy Configuration Report and the Vulnerability Assessment report, both of which are run only at the Administrator's discretion.

```
ironmail:
ironmail: run reports
*** Invalid command: Usage - run reports <MM/DD/YYYY> ***
ironmail:
ironmail: run reports 10/12/2004
Generating reports will highly impact the performance of the appliance. Are you sure? (Y/N) n
No report job submitted.
ironmail:
```

The SET Command

The **set** command is used to start, stop, enable and disable IronMail services, to configure the serial port, and to unlock user accounts that have been locked due to excessive failed login attempts. The **set** command accepts three parameters: **serial**, **service**, and **user unlock**. Once the user enters the command and first parameter, the screen displays a list of sub-parameters.

```
Command Summary:
set     serial     cli
                   ups
        service    enable     <SERVICE>
                   disable    <SERVICE>
                   start      <SERVICE>
                   stop       <SERVICE>
        user       unlock     <USERNAME>
        <SERVICE> = IronMail Services:
                    smtpproxy, smtpsproxy, smtpo, pop3proxy
                    pop3sproxy, imap4proxy, imap4sproxy, etc.
       <USERNAME> = IronMail User Account
```

The **set serial** command configures IronMail's serial port to do one of two things: to allow connection of a keyboard (console) directly to the appliance, using the **cli** sub-parameter; or to allow connection of an uninterruptable power supply, using the **ups** sub-parameter.

```
ironmail:
ironmail: set serial
*** Invalid command: Usage - set serial [cli|ups] ***

ironmail: set serial ups
The serial port is already set.

ironmail: set serial cli
Warning! The change may take up to 5 minutes ...
Serial port has changed.

ironmail: set serial ups
Warning! The change may take up to 5 minutes ...
Serial port has changed.
ironmail:
```

The **set service** command is used to enable, disable, start or stop an IronMail service.

Note: a disabled service cannot be started.

A service can also be disabled in the GUI by de-selected the Autostart option for that service.

```
ironmail:
ironmail: set service
*** Invalid command: Usage - set service [enable|disable|start|stop] ***
ironmail: set service enable
*** Invalid command: Usage - set service enable <SERVICE> ***
ironmail: set service disable
*** Invalid command: Usage - set service disable <SERVICE> ***
ironmail: set service start
*** Invalid command: Usage - server service start <SERVICE> ***
ironmail: set service stop
*** Invalid command: Usage - server service stop <SERVICE> ***
```

The set **user unlock <username>** command is used by the Administrator to unlock an appliance that has been locked due to circumstances like failed login attempts exceeding the maximum allowed. A valid username is required.

```
ironmail: set user
*** Invalid command: Usage - set user [unlock] ***
ironmail: set user unlock
*** Invalid command: Usage - set user unlock <USER ID> ***
ironmail:
```

The SHOW Command

The **show** command displays information about IronMail's system, services, *network* and logs. After the user types the command and the first parameter, the screen displays available sub-parameters.

```
Command Summary:
show    log     <SERVICE>
        mailroute
        network     connections
                    interface
                    route
        queue
        system      <SERVICE>
        services
        system      disk
                    process
                    support
To get more information on each of these commands, type 'help show log', 'help show services', or
'help show system'.
```

The **show log** command allows the Administrator to view today's logs, or those from a previous day.

```
ironmail: help show log
The 'show log' command is used to view today's, or previous days' logs.  To see the list of services
whose logs are available, type 'show log'.
To view today's logs for an individual service, type 'show log <SERVICE>' (where <SERVICE> is
one of the services displayed by the 'show log' command).  Appending a '?' after <SERVICE>
displays the dates for previous days' logs. Appending the date after <SERVICE> displays the log
for that day.
Examples:
        show log smtpproxy = Show today's smtpproxy log
        show log smtpproxy ? = Show dates for previous days' logs available
        show log smtpproxy 20040101 = Show the smtpproxy log from 1/1/2004
ironmail:
ironmail: show log
```

```
show log [adeladminlalertlavqlcfqlcleanuplct_adminlct_auditlct_euserleusrquarant
inelimap4proxylimap4sproxylironwebmaillljoinqlldapsynclmmqlpop3proxylpop3sproxylreportslripqlsc
hedl
schedftplsmtpolsmtpproxylsmtpsproxylspamqlsshdctllsummarylsuperqlvfqlwatch] <Date, ? for list,
Enter for today>
ironmail:
```

The **show mailroute** command displays information about the configured routing for various email protocols.

```
ironmail: show mailroute
*** Invalid command: Usage - show mailroute <IMAP4|POP3|SMTP> ***
ironmail: show mailroute IMAP4
Protocol        Routing Domain  Routing Host
--------        --------------  ------------
IMAP4           DEFAULT         mail.x3.ctqa.net
IMAP4           x3.ctqa.net     mail.x3.ctqa.net
ironmail:
```

The **show network** command shows details about network configuration.

```
ironmail: help show network
The 'show network' command is used to view network related information.
show    network connections
              interface
              route
ironmail: show network connections
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  localhost.22502       localhost.1212         ESTABLISHED
tcp4       0      0  localhost.1212        localhost.22502        ESTABLISHED
tcp4       0      0  localhost.3306        localhost.3218         ESTABLISHED
tcp4       0      0  localhost.3218        localhost.3306         ESTABLISHED
tcp4       0      0  localhost.3659        localhost.30340        TIME_WAIT
tcp4       0      0  im.1174               upd.ctqa.net.20022     TIME_WAIT
tcp4       0      0  localhost.22502       localhost.4192         TIME_WAIT
tcp4       0      0  localhost.2769        localhost.3306         TIME_WAIT
tcp4       0      0  localhost.22502       localhost.2688         TIME_WAIT
tcp4       0      0  localhost.2973        localhost.3306         TIME_WAIT
tcp4      74      0  im.4447               im.10443               CLOSE_WAIT
tcp4       0      0  localhost.8009        localhost.3337         ESTABLISHED
tcp4       0      0  localhost.3337        localhost.8009         ESTABLISHED
tcp4       0      0  localhost.8009        *.*                    LISTEN
tcp4       0      0  im.https              *.*                    LISTEN
tcp4       0      0  im.10443              *.*                    LISTEN
```

```
ironmail:
ironmail: show network interface
<PRIMARY> interface
  Attribute    Current        Pending
  =========    =======        =======
  IP Address   10.50.1.234     None
  Netmasks     255.255.255.0   None
  Media Type   None            None
  Status       active          None
<OOB> interface DISABLED
  Attribute    Current        Pending
  =========    =======        =======
  IP Address   None            None
  Netmasks     None            None
  Media Type   None            None
  Status       no carrier      None
ironmail:
ironmail: show network route
No static route record.
ironmail:
```

The **show queue** command displays configuration information about processing order.

```
ironmail: show queue
      Queue Position and Name
      ======================
   1  Internal Queues - MIME Ripper
   2  Internal Queue - Content Extraction
   3  Super Queue
   4  Queue - Anti Spam
   5  Queue - Virus Scan
   6  Queue - Mail Monitoring
   7  Queue - Content Filtering
   8  Internal Queue - MIME Joining
   9  SMTPO Service
ironmail:
```

The **show services** command displays the current status of IronMail's services.

```
ironmail: show services
Mail Processes
Service             Auto-Start      Running       Uptime(D:H:M:S)
=========================================================================
IronWebMail             Y             Y          0000:00:02:17
SMTPI Service           Y             Y          0000:22:51:44
SMTPIS Service          Y             Y          0000:22:51:44
SMTPO Service           Y             Y          0000:22:51:44
POP3 Service            Y             Y          0000:22:51:44
POP3S Service           Y             Y          0000:22:51:44
IMAP4 Service           Y             Y          0000:22:51:44
IMAP4S Service          Y             Y          0000:22:51:43
Queue Processes
Service             Auto-Start      Running       Uptime(D:H:M:S)
=========================================================================
Super Queue             Y             Y          0000:00:00:31
Misc Processes
Service             Auto-Start      Running       Uptime(D:H:M:S)
=========================================================================
CLI Access              Y             Y          0000:22:51:44
CipherTrust Support Ac     Y             Y          0000:04:56:10
Alert Manager           Y             Y          0000:22:51:42
Network IDS             Y             Y          0000:22:51:43
Anomaly Detection Engi     Y             Y          0000:22:51:40
Internal Processes
Service             Auto-Start      Running       Uptime(D:H:M:S)
=========================================================================
Int - Webadmin          Y             Y          0000:00:02:17
Int - Tomcat            Y             Y          0000:22:51:37
Int - Health Monitor       Y             Y          0000:22:51:39
Int - Reports           Y             Y          0000:12:27:05
Int - Scheduler         Y             Y          0000:22:51:42
Internal Queues - MIME     Y             Y          0000:22:51:42
Internal Queue - MIME      Y             Y          0000:22:51:42
Internal Queue - Conte     Y             Y          0000:22:51:42
ironmail:
```

The **show system** command string displays critical information about the IronMail system, including disk status and process statistics.

```
Command Summary:
show     system     disk
                     process
                     support

ironmail: show system disk
Mounted      Size     Used    Avail Capacity    iused    ifree   %iused
/ct          34G     1.3G      30G      4%    12129  8191645      0%
ironmail:

ironmail: show system process
Time     % User  % Sys  % Nice  % Intrpt  % Idle
00:00       5          0          0          0        95
00:01       6          0          0          0        94
00:04       3          2          0          0        95
00:05       3          2          0          0        95
00:06       4          0          0          0        96
00:06       4          2          0          0       94
00:07       4          1          0          1       95
00:08       5          1          0          0       94
00:09       7          0          0          0       93
ironmail:

ironmail: show system support
Support access is enabled.
Support access listen port has set to {port:20022}.
ironmail:
ironmail:
```

The show system process command shows a table similar to the one below.

Time	%User	%System	%Nice	%Intrpt	%Idle
00:02	1	2	0	0	98
00:17	3	1	0	0	96
00:32	2	0	0	0	98
00:47	2	1	0	0	97
Time	Every 15 minutes, IronMail takes a "snapshot" of its CPU utilization. IronMail's time within any 24 hour cycle is given.				
%User	This reports the percentage of CPU utilization for all IronMail processes running in User Space.				
%System	This reports the percentage of CPU utilization for all processes running in System Space.				
%Nice	This reports the percentage of CPU utilization for all processes running in Nice Space.				
%Intrpt	This reports the percentage of CPU utilization for all processes running in Interrupted Space.				
%Idle	This reports the percentage of CPU utilization waiting in an Idle state.				

The SYSTEM Command

The SYSTEM command is used to reboot/shutdown IronMail and restore IronMail's factory settings. (You may restore either the security certificate, network settings, or disable ACL on the WebAdmin.) Restoring factory settings can be used to recover when the Graphical User Interface of IronMail's Web Administration has become unavailable due to misconfiguration.

The **system** command accepts the following parameters: **shutdown reboot restart restore**.

Command Summary:

To Reboot/Shutdown system: system reboot
shutdown

To Restart Webadmin: system restart webadmin

To Restore Factory Settings: system restore acl
certificate
network

The TAIL Command

The **tail** command shows a real-time view of all IronMail logs, beginning with the 10 most recent entries. The command accepts the parameter: **log** The tail command accepts no additional switches.

The **tail log** command accepts the additional parameters of the names of IronMail logs. Typing **tail log** will reveal a list of all available logs.

```
Command Summary:
tail    log  <SERVICE>
ironmail: tail log
tail log
[adeladminlalertlavqlcfqlcleanuplct_adminlct_auditlct_euserleusrquarantinelimap4proxylimap4spro
xylironwebmaill
joinqlldapsynclmmqlpop3proxylpop3sproxylreportslripqlschedlschedftplsmtpolsmtpproxylsmtpsproxy
lspamql
sshdctllsummarylsuperqlvfqlwatch] <Date, ? for list, Enter for today>


ironmail:
ironmail: tail log cfq
Channel2::6:10122004 15:14:50:LOG_STAT_FINALl6lPUSHED TO NEXT Q
Channel3::7:10122004 15:15:20:LOG_STAT_ATT_FIL: {}
Channel3::7:10122004 15:15:20:LOG_STAT_CONT_FIL: {}
Channel3::7:10122004 15:15:20:LOG_STAT_FINALl7lPUSHED TO NEXT Q
Channel4::8:10122004 16:48:25:LOG_STAT_ATT_FIL: {}
Channel4::8:10122004 16:48:25:LOG_STAT_CONT_FIL: {}
Channel4::8:10122004 16:48:25:LOG_STAT_FINALl8lPUSHED TO NEXT Q
Channel5::9:10122004 17:05:07:LOG_STAT_ATT_FIL: {}
Channel5::9:10122004 17:05:07:LOG_STAT_CONT_FIL: {}
Channel5::9:10122004 17:05:07:LOG_STAT_FINALl9lPUSHED TO NEXT Q
```

The TEST Command

The **tes**t command is used to test network connections by using different methods, as well as to check specific server connections. The **test** command accepts the following parameters: **dns mail ping port route server**.

Examples are shown below:

```
Command Summary:
test    dns      forward <DNS SERVER IP> <HOSTNAME>
                 mx      <DNS SERVER IP> <DOMAIN NAME>
                 reverse <DNS SERVER IP> <IP ADDRESS>
        mail     <MAIL SERVER IP> <SENDER> <RECIPIENT>
```

```
        ping     <HOST>
        port     <IP ADDRESS> <PORT>
        route    <DOMAIN NAME>
        server   rlb <IP ADDRESS> <RBL SERVER> <DNS SERVER IP> <QUEUE TYPE>
                 sls
                 update
ironmail:
ironmail: test server sls
# 10/13/04 11:42:01 EDT  /ct/apps/sls/client/conf/map
# Re-resolve names after 13:41:56  Check RTTs after 11:57:01
# 8000.00 ms threshold, -8000.00 ms average    1 total, 1 working addresses
IPv6 off
sls1.ciphertrust.net,-      123789 client101
# * 10.50.1.16,-                              qa1.DCC.ciphertrust ID 1040
#     100% of 32 requests ok   10.85 ms RTT            6 ms queue wait
```

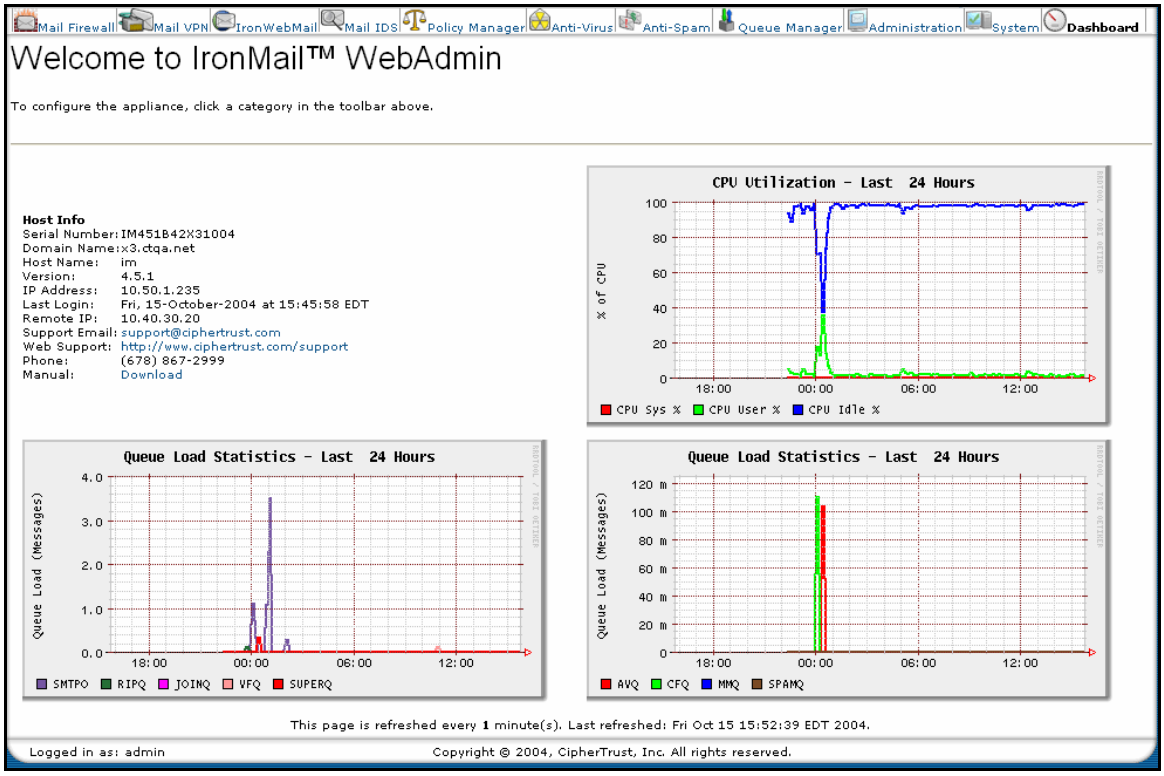
WATCHING THE SYSTEM

Monitoring Conditions

IronMail provides the Administrator accurate status information through two different means: both configurable and non-configurable graphs providing utilization information at a glance; and the Dashboard, providing current statistic information on one screen. The non-configurable graphs appear when one logs into IronMail.

Opening Graphs

When IronMail opens, the screen shown below appears. It includes by default three graphs that indicate CPU utilization and the load statistics for eight different queues, for the past 24 hours. These graphs are not configurable.



To access the System Graphs or Queue Graphs, click the ***Graphical Analysis*** tab at the top of the screen. One group of the configurable graphs or the Dashboard will display.

Graphical Analysis

Reporting Utilization

IronMail provides the Administrator beneficial graphic information regarding the current status of tools and processes and system utilization. This data provides useful data for capacity planning purposes and can signal the administrator events requiring attention. The information is displayed in the opening series of graphs when one logs into IronMail, and in configurable process and system graphs accessible from the IronMail screen.

The information for the graphs is gathered from the Dashboard area. Data are reported regarding:

- CPU
- memory
- disk
- file systems
- network throughput
- queue load
- queue totals
- queue actions

The information on the process and system graphs may be displayed for specific time spans as desired. Configuration is simple, and will be shown for the specific types of graphs. The graphs will show data for the following intervals:

- the past hour
- the past three hours
- the past twelve hours
- the past 24 hours
- the past 7 days
- the past 30 days
- the past 90 days

This configuration option allows the Administrator to analyze trends, etc., over variable time periods. .

While the data intervals to be graphed are configurable, the actual data is sampled each minute. The resulting information is accumulated, to be shown appropriately in the graphic representations. Collected data accumulates as follows, and is rolled up (via averaging) after the specified number of observations:

- 300 observations at one-minute intervals
- 288 observations at ten-minute intervals
- 336 observations at 30-minute intervals
- 360 observations at 120-minute intervals (every two hours)
- 270 observations at 480-minute intervals (every eight hours)
- 365 observations at 1440-minute intervals (once per day)

This accumulation system allows IronMail to draw upon whatever groups of observations necessary to prepare the graphs indicated by the time-span configuration, as well as ensuring that the data set does not grow beyond a pre-determined limit.

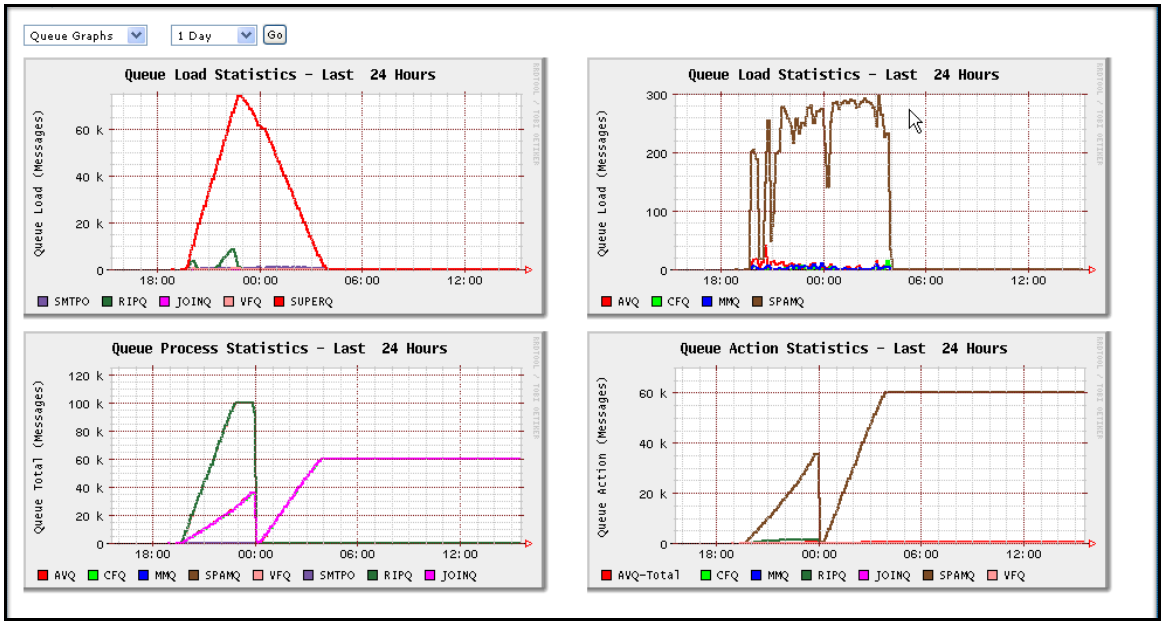
The Queue Graphs and System Graphs presented on the screens, as shown below, will automatically refresh on a pre-configured cycle. However, the opening graphs that are visible when the user logs into IronMail will NOT refresh on that same cycle. Instead, they will refresh as the screen opens. Details of IronMail processing are tracked in the Queue Graphs and System Graphs.

Queue Graphs

This group of graphs can be selected by choosing "Queue Graphs" from the drop-down list at the upper left of the screen. The same choice is available on the "System Graphs" screen, as well, allowing you to toggle back and forth between the groups. The time interval you wish the graphs to cover is configurable for each group by simply choosing an interval (from one hour to 90 days) from the second drop-down list. The examples below show data for the past hour.

The top two graphs in the group show the load statistics in terms of the number of messages presently in each of eight queues. Viewing two graphs rather than one makes it easier to follow the lines for each queue, with system queues on the left and user-configurable queues on the right. The lower graph on the left displays the total messages processed by each of the queues (cumulative totals) ***in a given 24 hour period from midnight to midnight***. The lower right graph shows the numbers of messages each queue has acted upon during this same time, ***again for a 24 hour period from midnight to midnight***.

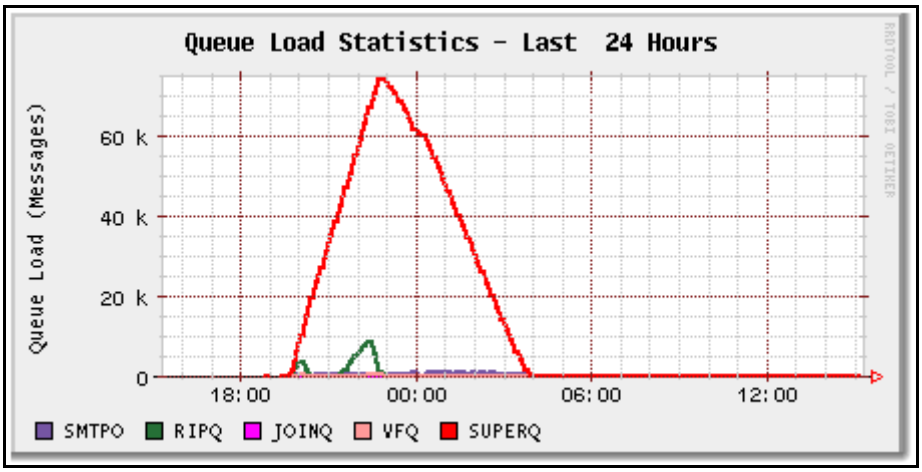
Note: The upper graphs (queue load) show the "point-in-time" count of messages for each queue, and the number will increase and decrease over time. The lower graphs (queue action and process statistics) show the cumulative message statistics for the current midnight-to-midnight period, and will only increase over this period. At midnight, these graph counters reset to zero for the next day.

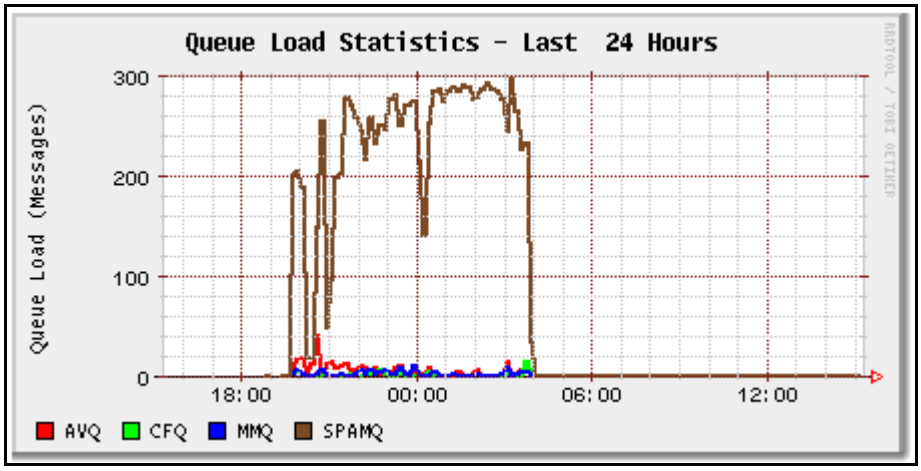


A more detailed look at each graph follows.

Queue Load Statistics

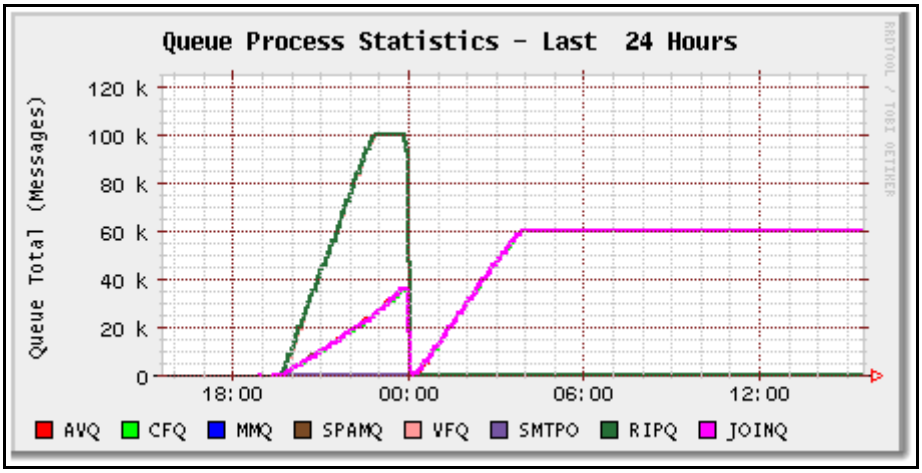
The top two graphs in the Queue Graphs group show the load statistics for each of the eight queues in IronMail. The graph to the left shows loads for SMTPO (the Outbound Queue), RIPQ, JOINQ, and VFQ (the Content Extraction Queue). The graph to the right shows loads for AVQ (Anti-Virus), CFQ (Content Filtering), MMQ (Mail Monitoring) and SPAMQ (the Spam Queue). The graphs show the number of messages being processed by each of these queues at a given point in time. In these examples, the graphs cover the past hour.





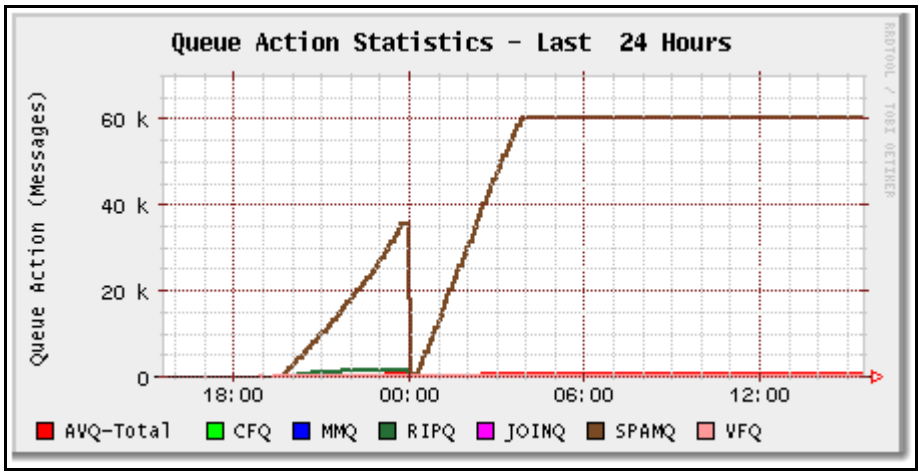
Queue Process Statistics

The graph to the lower left shows Queue Process statistics for the configured time period (in this case, one hour). However, as indicated above, the information presented is cumulative over the current 24-hour period, from midnight to midnight. The graph is reset to zero at midnight.



Queue Action Statistics

The final graph in this group shows the number of messages being acted upon by IronMail for the configured time period (one hour again, in this instance). This data is also cumulative, and increases over the time period from midnight to midnight. This graph is also reset at midnight.



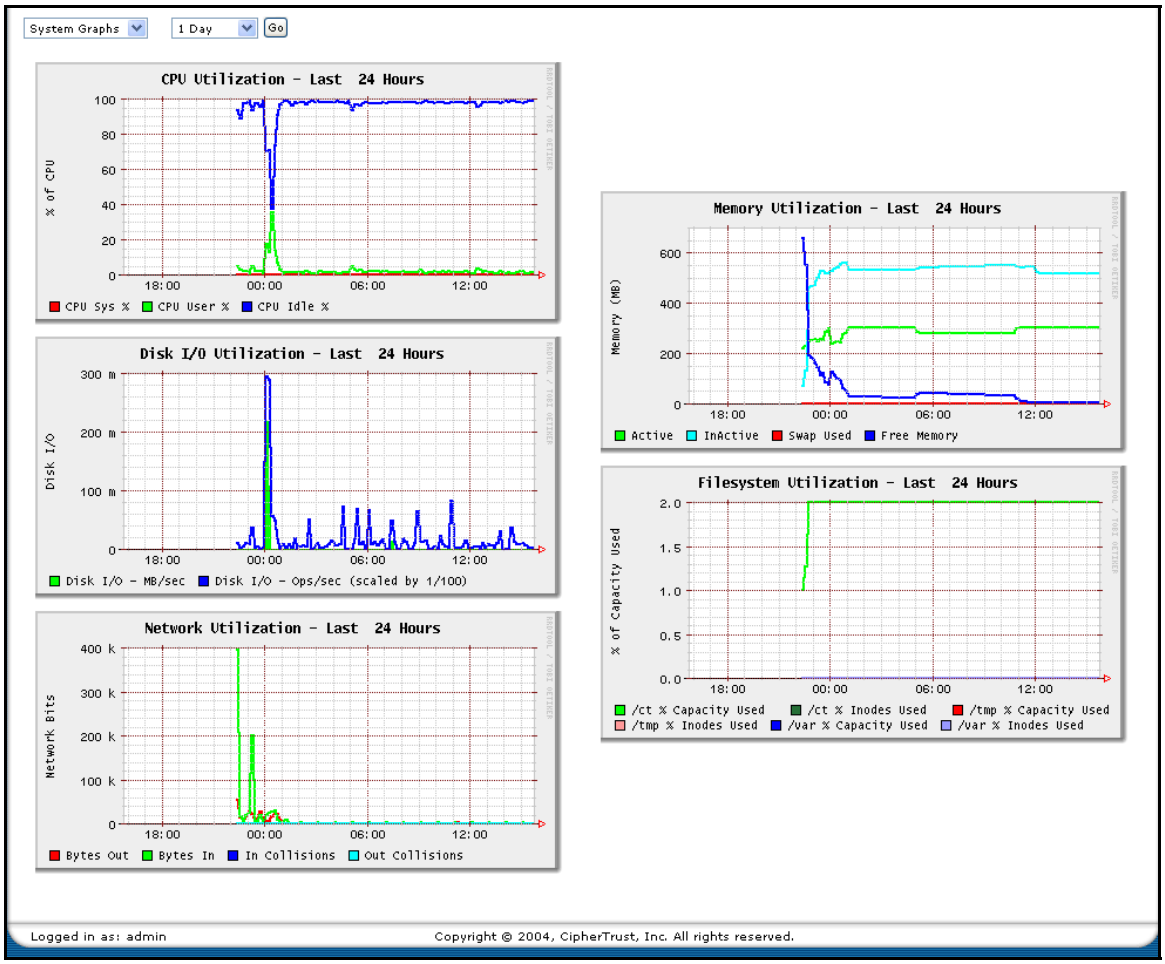
Selecting "System Graphs" from the drop-down list closes this screen and opens the other set of graphs.

System Graphs

This group of graphs can be selected by choosing "System Graphs" from the drop-down list at the upper left of the screen. The same choice is available on the "Queue Graphs" screen, as well, allowing you to toggle back and forth between the groups. The time interval you wish the graphs to cover is configurable for each group by simply choosing an interval (from one hour to 90 days) from the second drop-down list. The examples below show data for the past hour.

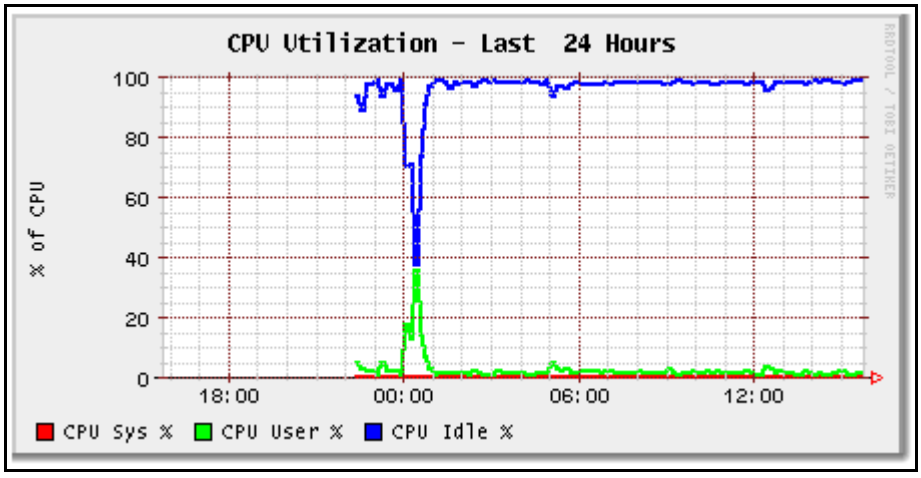
The graphs in this group display the following information:

- The upper left graph shows CPU utilization in percentage of capacity
- The upper right graph shows memory utilization in megabytes
- The middle left graph displays disk utilization in terms of input and output operations
- The middle right graph displays file system utilization in percentage of capacity
- The bottom right graph shows *network* utilization in network bits.



CPU Utilization:

The upper left graph shows CPU utilization in percentage of capacity. The total of all three percentages should yield 100%.



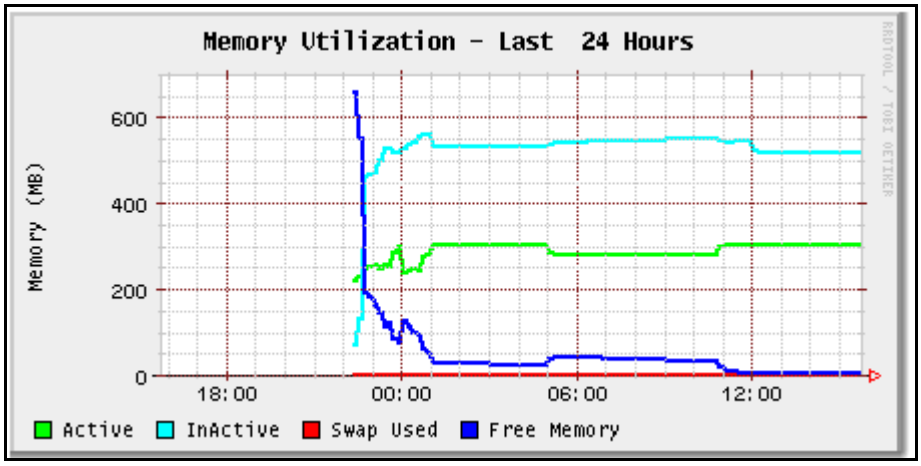
The graph tracks the following information:

- Idle – this line tracks the percentage of CPU capacity that was not in use at a given point in time during the period covered by the graph (in this case, one hour).

- User –this line represents the percentage of CPU capacity that was in use at the Application level (being used by one or more applications) at a given point in time.
- Sys – this line presents the percentage of CPU capacity that was in use at the System level (being used by the system to support the applications in use) at a given point.

Memory Utilization

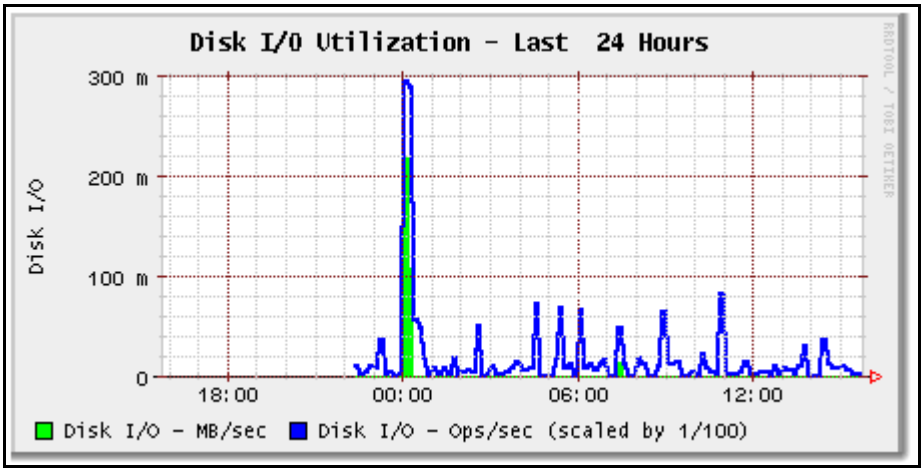
The upper right graph shows memory utilization in megabytes.



- Active – This line represents the megabytes of memory being actively used at any given point over the configured time span (one hour, in this example).
- Inactive – This line tracks the megabytes of memory that have been in use and are not in active use at this point, but that have not been released to become free memory.
- Free – The free memory line shows the megabytes of memory available for use by any initiated process at a given point in time.
- Swap Used – This line only becomes active when no free memory exists (free memory = 0). It traces the number of megabytes of information that have been temporarily transferred to disk in order to free up memory for use.

Disk Input/Output Utilization

This graph displays disk usage data regarding number of megabytes per second and the number of input/output operations per second.

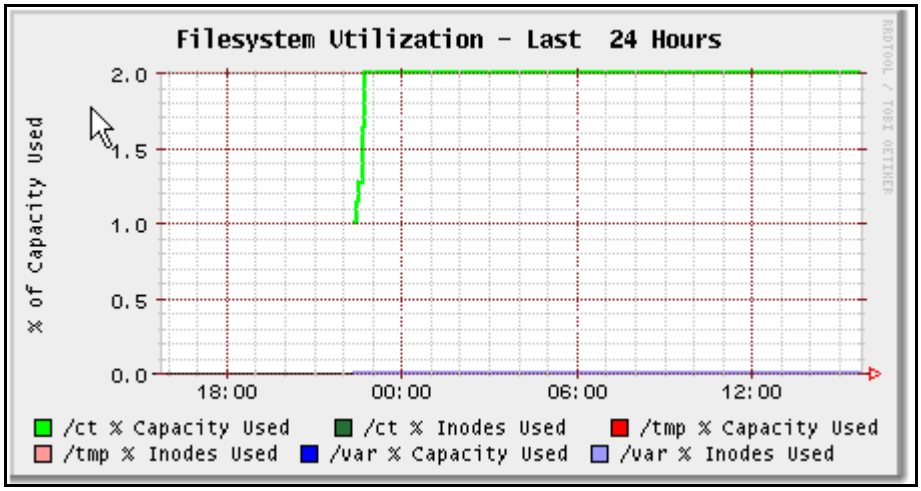


The middle left graph displays disk utilization in terms of input and output operations

- MB/second – this portion of the graph indicates the number of megabytes per second of data transfer into or out of the disk at any given point.
- Operations/second/100 – this line follows the number data input and/or output operations per second at any point scaled by dividing by 100. The actual number is 100 X the number displayed on the graph.

File System Utilization

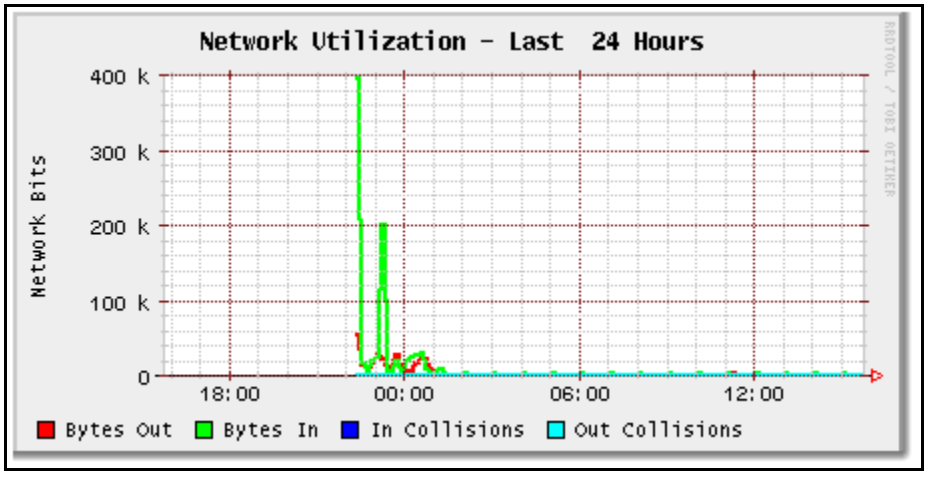
The middle right graph displays file system utilization in terms of the percentage of capacity used and the percentage of available inodes used. Each parameter is tracked for three separate partitions on the file system: /ct, /var, and /tmp.



- % capacity used – these lines represents the percentage of capacity in use by the partitions at any given point in time over the configured span (one hour in this example).
- % inodes used – these lines represent the percentage of available inodes in use by the partitions at any given point in time over the configured span.

Network Utilization

The bottom right graph shows network utilization (input and output) in bits/second.



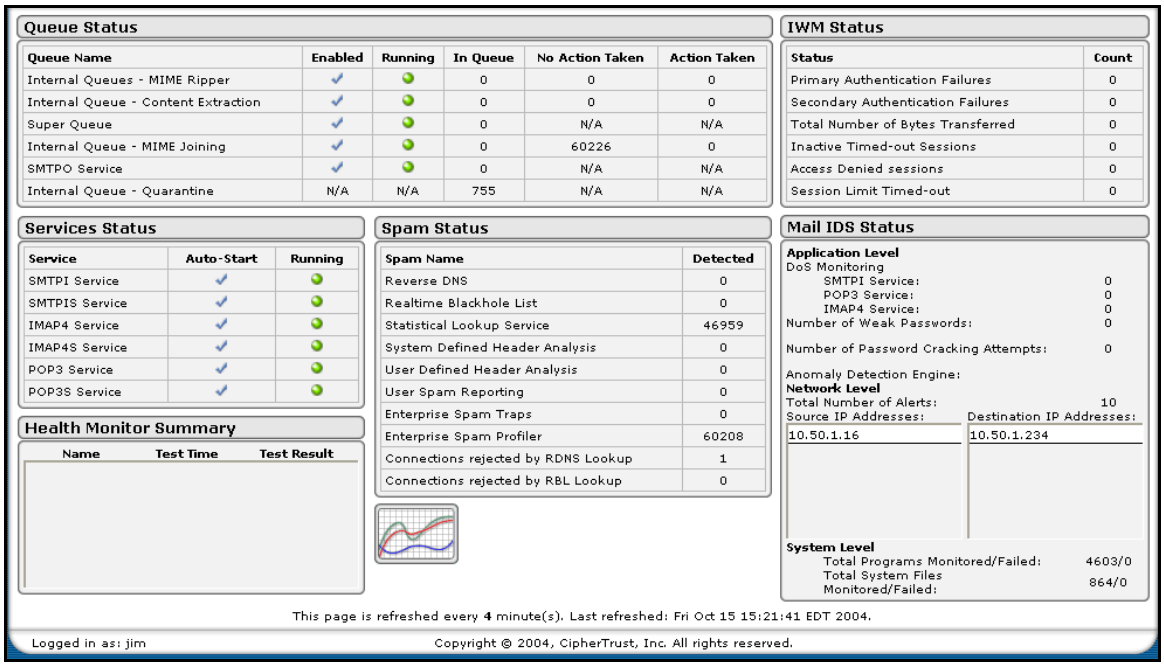
- BitsBytes out – this line shows the number of bytes of outbound data on the network at any given point.

- BitsBytes in - this line tracks the number of bytes of inbound data on the network at any given point.
- Collisions Out – the line represents the number of outbound bytes of data in requests to resend information that was not successfully received.
- Collisions In – this line shows the number of bytes of data being re-received by the network.

Statistical Analysis

The Dashboard

IronMail's "Dashboard" is a "one-screen-shows-it-all" interface that allows the Administrator to quickly see the status of all its systems. The information displayed there is both cumulative and static. *Each time the page is refreshed, IronMail's current settings are updated.* The Dashboard refreshes at four-minute intervals, so the information displayed is always current.


Queue Status
Queue Name | Enabled | Running | In Queue | No Action Taken | Action Taken
Internal Queues - MIME Ripper | 0 | 0 | 0
Internal Queue - Content Extraction | 0 | 0 | 0
Super Queue | 0 | N/A | N/A
Internal Queue - MIME Joining | 0 | 60226 | 0
SMTPO Service | 0 | N/A | N/A
Internal Queue - Quarantine | N/A | N/A | 755 | N/A | N/A
IWM Status
Status | Count
Primary Authentication Failures | 0
Secondary Authentication Failures | 0
Total Number of Bytes Transferred | 0
Inactive Timed-out Sessions | 0
Access Denied sessions | 0
Session Limit Timed-out | 0
Services Status
Service | Auto-Start | Running
SMTPI Service
SMTPIS Service
IMAP4 Service
IMAP4S Service
POP3 Service
POP3S Service
Spam Status
Spam Name | Detected
Reverse DNS | 0
Realtime Blackhole List | 0
Statistical Lookup Service | 46959
System Defined Header Analysis | 0
User Defined Header Analysis | 0
User Spam Reporting | 0
Enterprise Spam Traps | 0
Enterprise Spam Profiler | 60208
Connections rejected by RDNS Lookup | 1
Connections rejected by RBL Lookup | 0
Mail IDS Status
Application Level
DoS Monitoring
SMTPI Service: 0
POP3 Service: 0
IMAP4 Service: 0
Number of Weak Passwords: 0
Number of Password Cracking Attempts: 0
Anomaly Detection Engine:
Network Level
Total Number of Alerts: 10
Source IP Addresses: Destination IP Addresses:
10.50.1.16 10.50.1.234
System Level
Total Programs Monitored/Failed: 4603/0
Total System Files Monitored/Failed: 864/0
Health Monitor Summary
Name | Test Time | Test Result
This page is refreshed every 4 minute(s). Last refreshed: Fri Oct 15 15:21:41 EDT 2004.
Logged in as: jim
Copyright © 2004, CipherTrust, Inc. All rights reserved.

The various Dashboard status fields have their data reset depending on the type of status information reported. The Policy Status and Spam Policy Status are reset nightly at 12:30.

The Mail IDS Status and IronWebMail Status numbers contain information accumulated in the last "cleanup interval" (the aging setting for the number of hours until they are cleaned up). This is not reset daily. The values seen on the Dashboard window accumulate and are cleaned up according to the cycle for the file type "Database" on the administrator controlled Cleanup Schedule.

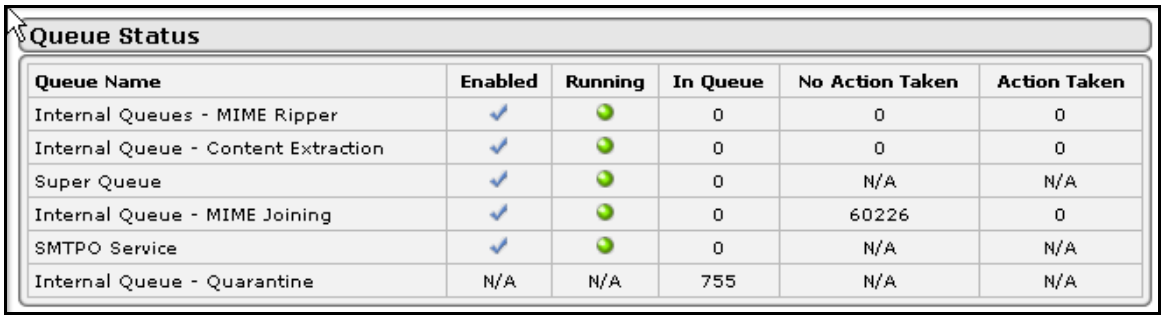
You cannot modify the configuration (enable, disable, etc.) any of the items in the Dashboard; the Dashboard only reports current status. Configuration must be done at the level of the individual service or tool.

The following information is available:

- Queue Status
- Spam Status
- Health Monitor Status

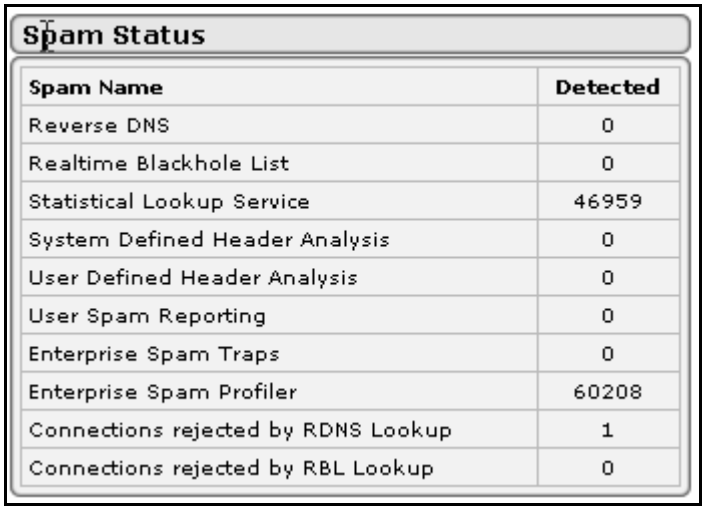
- Services Status
- IronWebMail Status
- Mail IDS Status

Queue Status



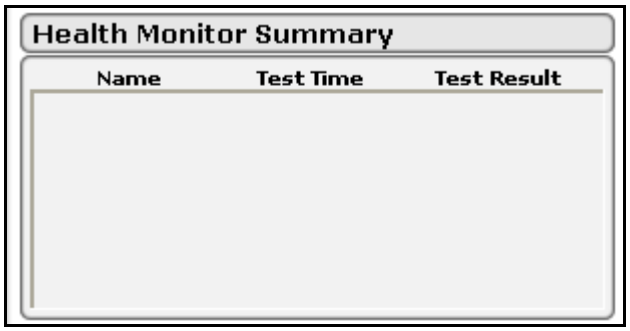
Queue Status provides a review of the current condition of each IronMail queue. The Administrator can see which queues are enabled and which are running, the number of messages currently in each queue, and the total numbers of messages that have been acted upon and that have passed through IronMail without action.

Spam Status



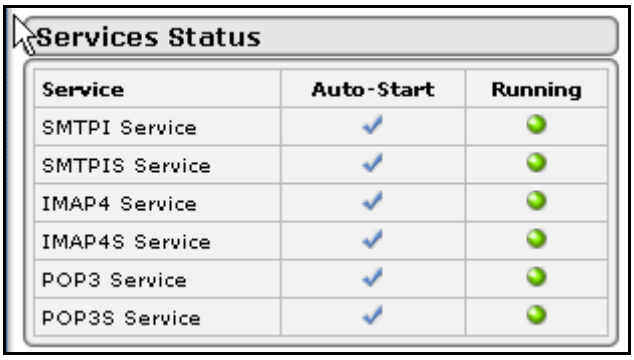
Spam Status is a summary of activity by each spam-blocking tool. The number of messages suspected of containing spam shows in the Detected column next to the associated tool.

Health Monitor Summary



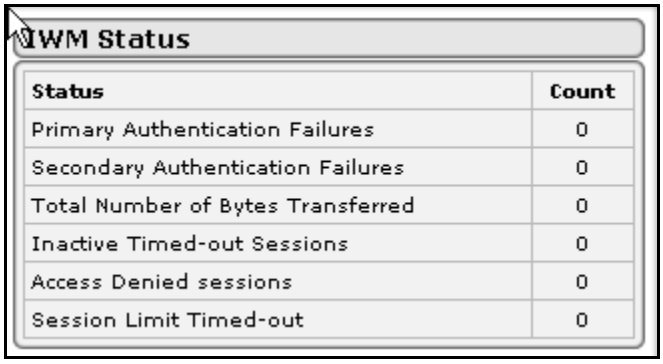
The Health Monitor Summary shows the tests run by the Health Monitor, the time for the last instance of each test, and a summary of the results for each test.

Services Status



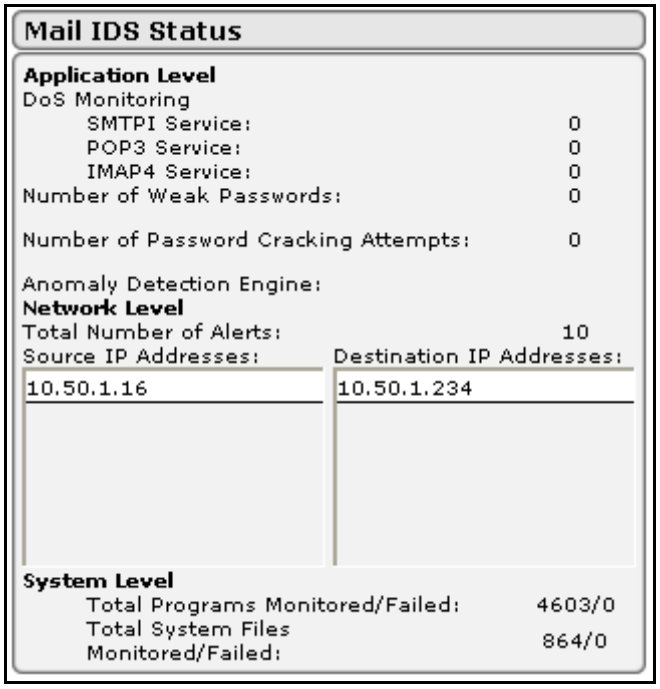
The Services Status table displays the current status of each of IronMail's services, allowing the Administrator to see at a glance which services are running and which are configured to be started automatically when the Health Monitor runs.

IronWebMail Status



This table records the current stats of IronMail's IronWebMail service, displaying pertinent statistics.

Mail IDS Status



The information displayed in the Mail-IDS Status table reflects IronMail's Mail-IDS tools, as configured in the Mail-IDS functional area. For each tool, the Dashboard reports a count for its associated IDS events.

CUSTOMIZING PAGES

Customizing IronMail Pages

An enterprise that use IronMail may desire to see some of the user-facing pages display a look and feel that reflects that enterprise's company identity. IronMail provides options to allow the Administrator to customize specific screens by adding logos, adding images, customizing text, etc. Both images and text may be added to specific screens for the following functional areas:

- IronWebMail (IWM)
- Secure Web Delivery (SWD)
- End User Quarantine (EUQ)

Each has its particular, unique pages to customize, but all are generally customized in the same way. Each customizable screen is delivered with the essential information and functionality in place; the essential information and fields in some pages, such as the IWM page, may not be changed with the exception of modifications to the fonts, the text colors, etc. In other pages, especially the ones that use tables, such as EUQ, the Administrator may remove, rename or reorder the information.

Customization involves three essential components: the customizable pages themselves, the proper cascading stylesheet (CSS) associated with each page, and the HTML template for each customizable page.

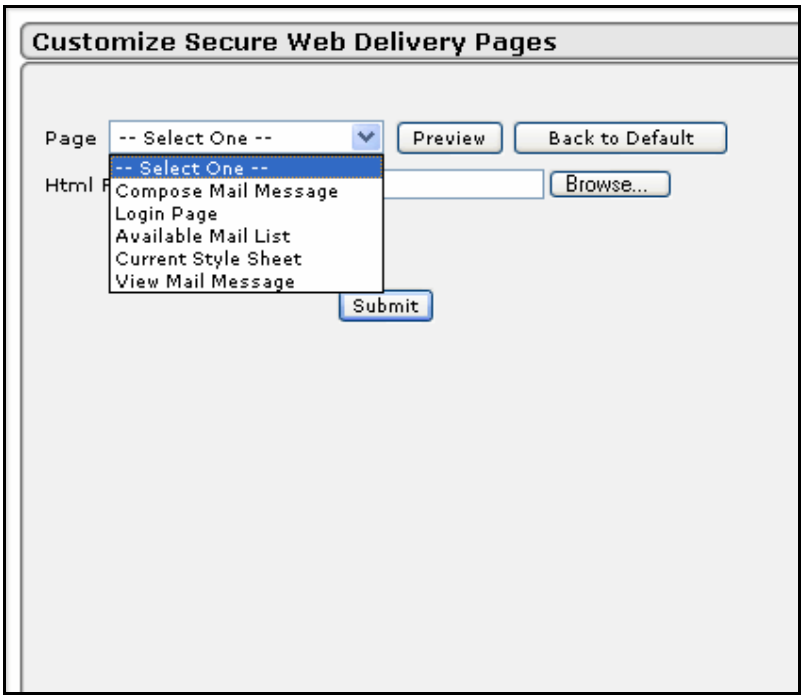
Note: The customization of the screens should be performed by a Developer or Administrator who has a good working knowledge of HTML. The actual customizations require changes to the templates for the specific pages.

Customizable Pages

Customization begins from a special screen in each of the three areas. These screens allow the Administrator to specify which page is to be customized, to manage images that may be used, to review the current appearance of the pages, and to access the stylesheets.

Customizing SWD

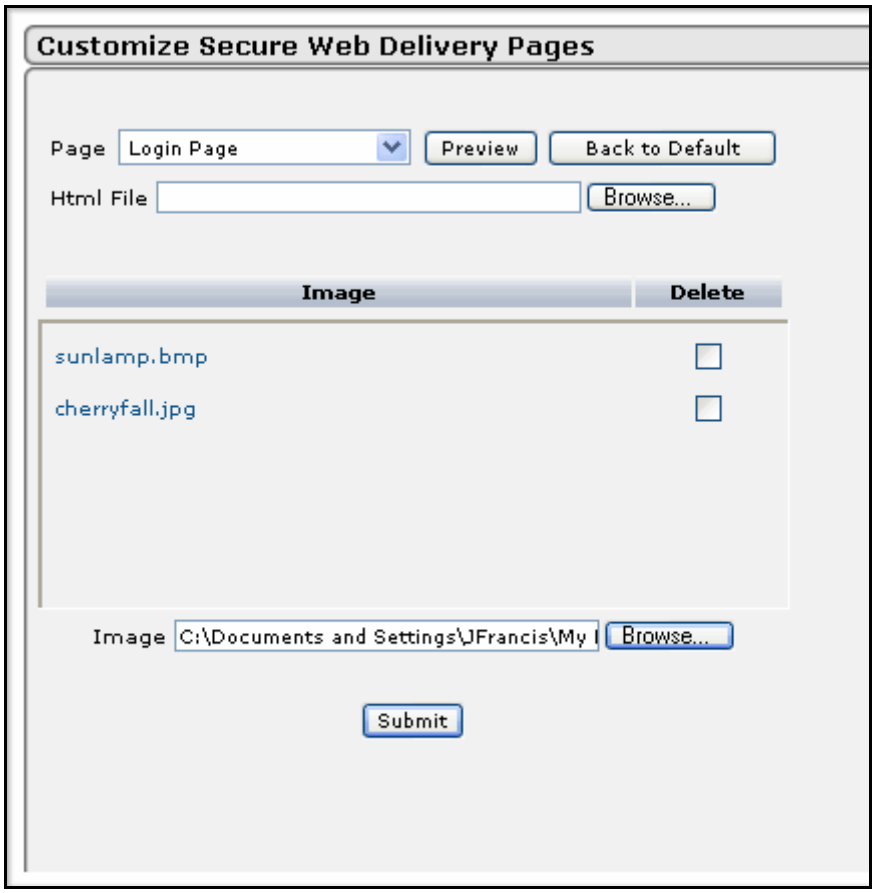
To begin customization for SWD, navigate to the Customize Secure Web Delivery Pages screen (*Secure Delivery > Secure Web Delivery > SWD Customize Pages*).



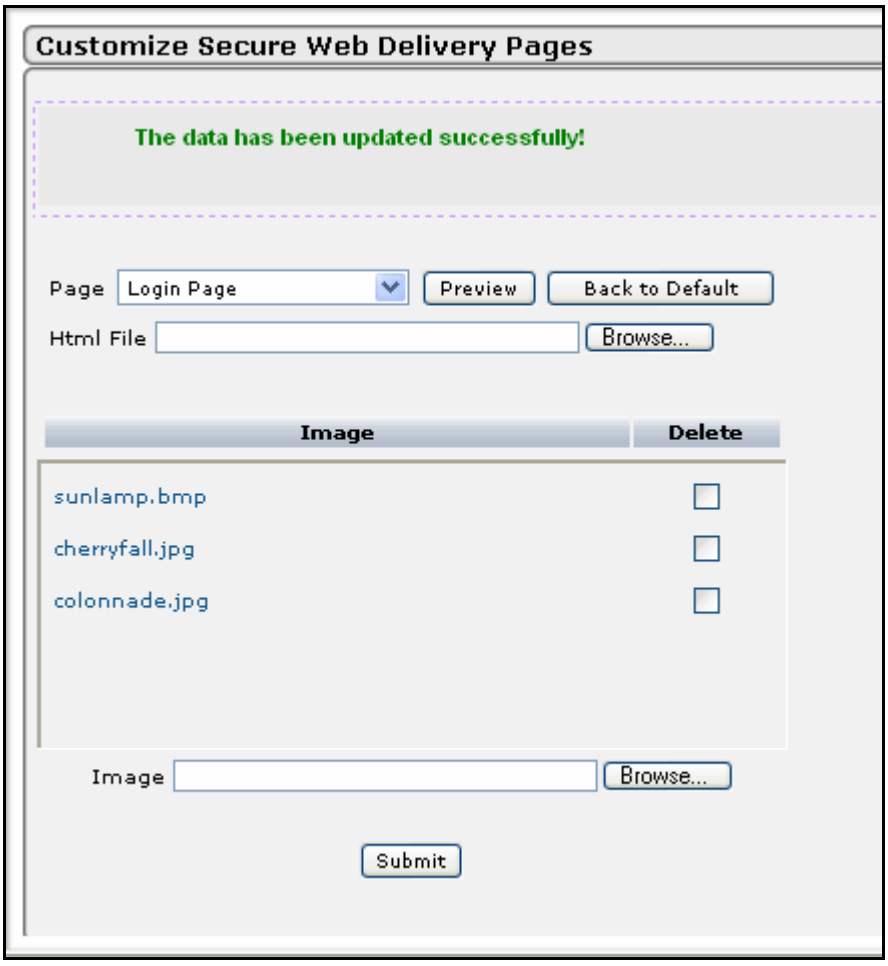
The screen provides the necessary fields to customize various pages.

Field	Description
Page	From the pick list, select one of the four customizable pages: • Compose Mail Message • Login Page • Available Mail List • View Mail Message You may also select the Current Style Sheet from the list.
Navigation Buttons	Two buttons beside the Page pick list allow you to: • **Preview** the selected page as it now appears, or see the current stylesheet. • Navigate **Back to Default** status. The selected page will return to its original status as it was before any customization was performed. All prior customizations will be lost.
HTML File	The field allows entry of the name and navigation path for an HTML file to be used, or you may navigate to the file using the Browse button.
Image Table	***After a page is selected, the table at the lower portion of the screen lists images available for use.***
Image	This column lists the names of images with their image type extensions. The image names may not have any spaces or special characters. The only image types that may be used are .gif, .jpg/jpeg or .bmp files. The images are stored in HTML files as /images/iwm/<image name>.
Delete	Each image has a delete button that allows removing it from the image table.
Image (data field)	You may enter the name of an image and it's complete navigation path in the field, or you may navigate to the image using the Browser button.

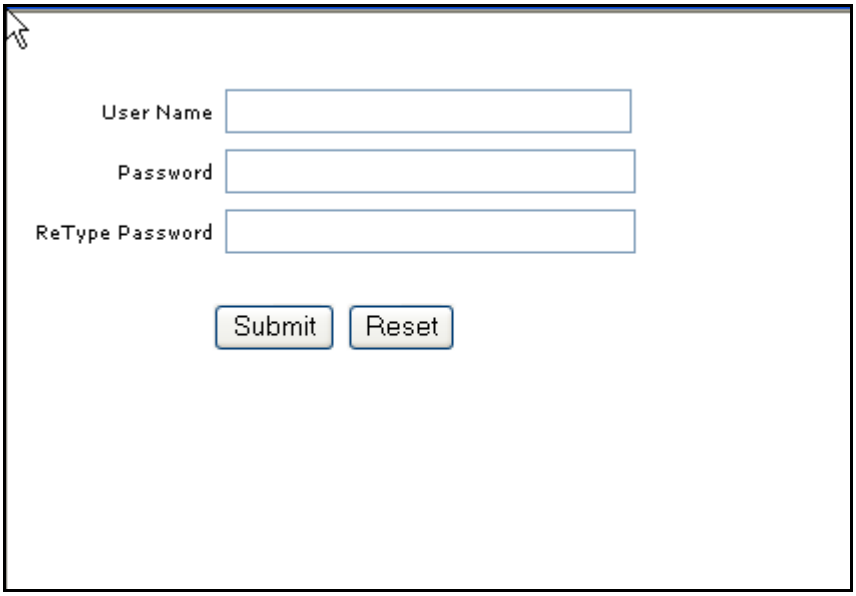
Click Submit to record changes. The images or HTML files will be available for use in the customization process.



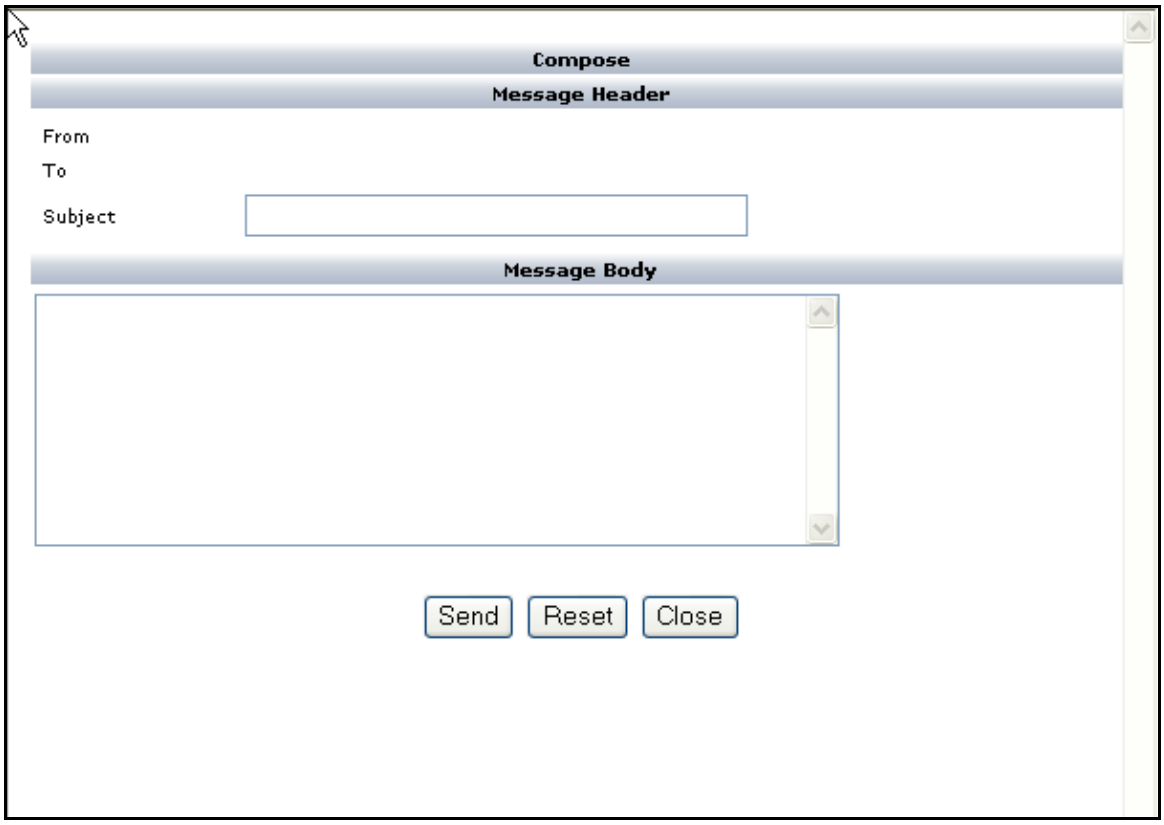
The screen shot above shows the customizing screen for the SWD Login page. Whenever one selects an image or file to add and submits the selection, the screen updates.



Clicking the Preview button for the Login screen before any customization is done opens the default screen configuration. If Back to Default is clicked, the login screen returns to this state.

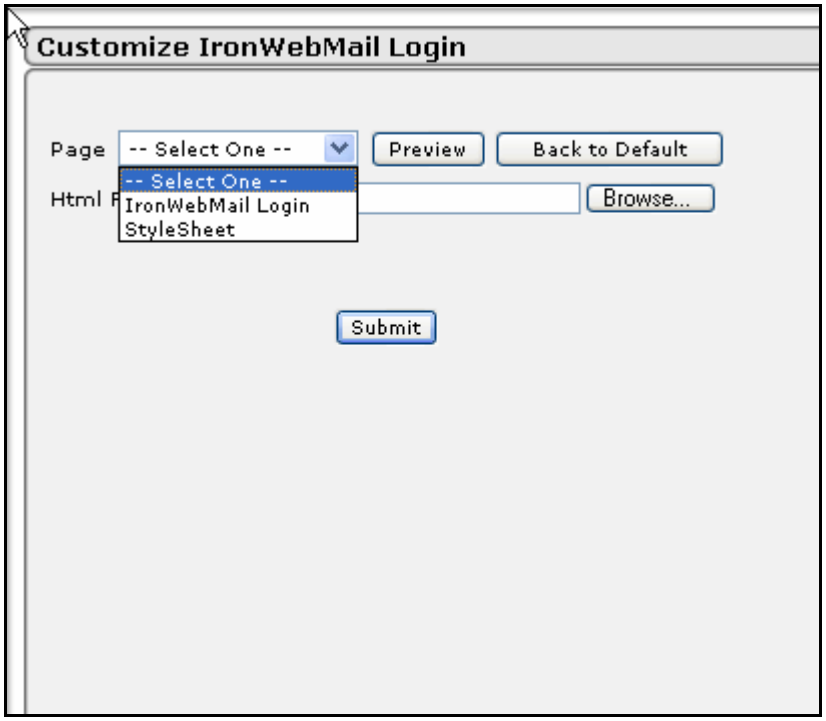


The default Compose Mail Message screen is shown below.


Compose
Message Header
From
To
Subject
Message Body
Send
Reset
Close

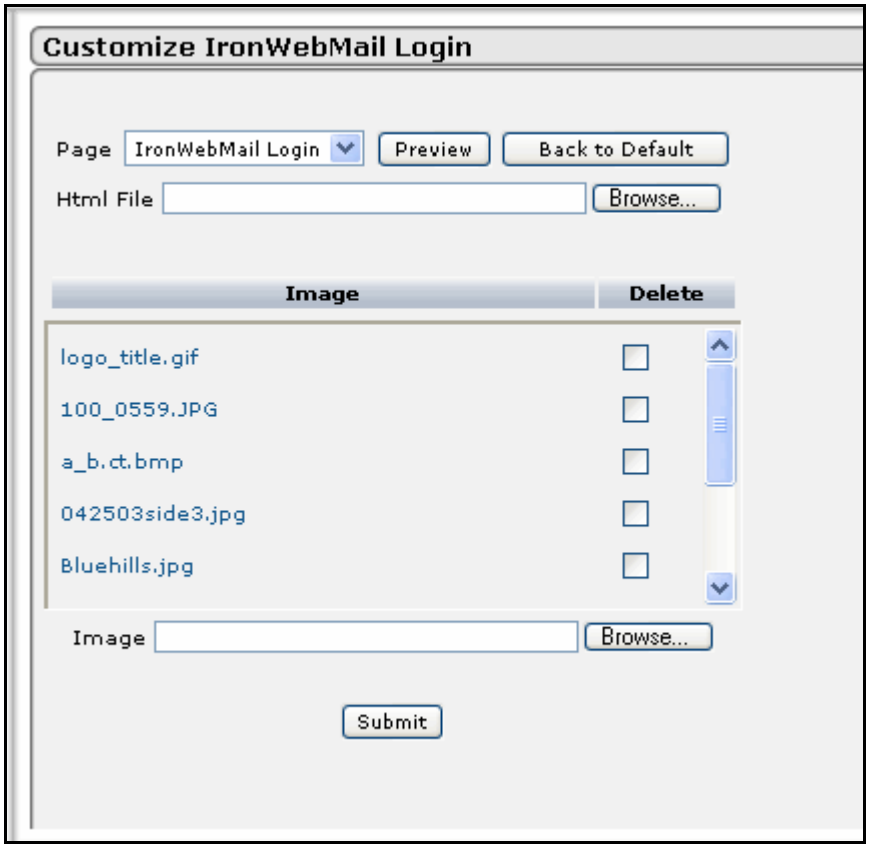
Customizing IWM

The IronWebMail Login screen may be customized using the options in the window below (*IronWebMail > IWM Customized Login*).



Field	Description
Page	From the pick list, select IronWebMail Login (this is the only page in this functional area that may be customized). You may also select the Current StyleSheet from the list.
Navigation Buttons	Two buttons beside the Page pick list allow you to: • **Preview** the selected page as it now appears, or see the current style sheet. • Navigate **Back to Default** status. The selected page will return to its original status as it was before any customization was performed. All prior customizations will be lost.
HTML File	The field allows entry of the name and navigation path for an HTML file to be used, or you may navigate to the file using the Browse button.
Image Table	***Afterthe page is selected, the table at the lower portion of the screen lists images available for use.***
Image	This column lists the names of images with their image type extensions. The image names may not have any spaces or special characters. The only image types that may be used are .gif, .jpg/jpeg or .bmp files. The images are stored in HTML files as /images/iwm/<image name>.
Delete	Each image has a delete button that allows removing it from the image table.
Image (data field)	You may enter the name of an image and it's complete navigation path in the field, or you may navigate to the image using the Browser button.

Select IronWebMail Login from the drop-down list, then click **Submit**.

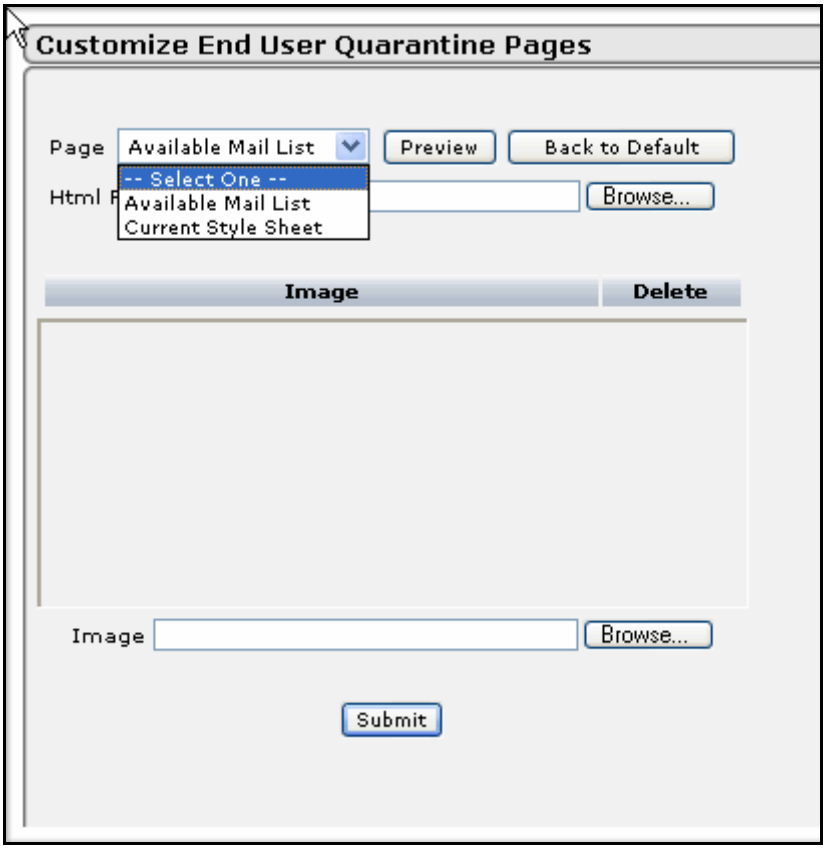


Images can be added to the list of available images by entering the name and complete path to the image or by browsing to the location where the desired image is stored, selecting it, and clicking **Submit**.

The actual customizations are performed by modifying the stylesheet. An example of a customized IWM Login page is shown below.

Customizing EUQ

Use the options in the screen below to customize the list of quarantined email messages intended for the recipient (*Policy Manager > End User Quarantine > Configure Web Page*).



Field	Description
Page	From the pick list, select Available Mail List, the only customizable page for End User Quarantine. You may also select the Current Style Sheet from the list.
Navigation Buttons	Two buttons beside the Page pick list allow you to: • **Preview** the selected page as it now appears, or see the current stylesheet. • Navigate **Back to Default** status. The selected page will return to its original status as it was before any customization was performed. All prior customizations will be lost.
HTML File	The field allows entry of the name and navigation path for an HTML file to be used, or you may navigate to the file using the Browse button.
Image Table	***After a page is selected, the table at the lower portion of the screen lists images available for use.***
Image	This column lists the names of images with their image type extensions. The image names may not have any spaces or special characters. The only image types that may be used are .gif, .jpg/jpeg or .bmp files. The images are stored in HTML files as /images/iwm/<image name>.

Delete	Each image has a delete button that allows removing it from the image table.
Image (data field)	You may enter the name of an image and it's complete navigation path in the field, or you may navigate to the image using the Browser button.

Clicking the Preview button before any customization is attempted displays the default Available Mail List.

Cascading Stylesheets

Cascading stylesheets determine the actual look and feel of the customized IronMail screens. A stylesheet is essentially a standardized template that assures uniformity from screen to screen among the enterprise's customized pages. Each of the three areas has a default stylesheet supplied by CipherTrust. An Administrator who is conversant with HTML can perform the specific customizations from these stylesheets or on a one-to-one basis from the HTML templates.

SWD Stylesheet

swm_customstyle[1].css

```
TD {
    font-family: verdana,helvetica,arial;
    font-size: 9px;
    color: black;
}

TH {
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    font-weight: bold;
    color: black;
    background-image : url('/images/thbackground.gif');
}

A {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}

A:visited {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}

A:hover {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}


BUTTON {
    font-family: verdana,helvetica,arial;
    font-weight: bold;
    font-size: 9px;
    color: black;
    padding-left:0px;
    padding-right:0px
}


.propertyEven {
    background-color: #ffffff;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}

.propertyOdd {
    background-color: lightgrey;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}
```

IWM Stylesheet

iwm_customstyle[1].css

```
body {
background-image:
url('/images/iwm/orangehills.jpg')
}

TD {
    font-family: verdana,helvetica,arial;
    font-size: 20px;
    color: blue;
}

TH {
    font-family: verdana,helvetica,arial;
    font-size: 20px;
    font-weight: bold;
    color: red;
    background-color: red;
}

A {
  font: 20px verdana, sans-serif;
  color: #green;
  text-decoration: none;
}

A:visited {
  font: 20px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}

A:hover {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}


BUTTON {
    font-family: verdana,helvetica,arial;
    font-weight: bold;
    font-size: 9px;
    color: black;
    padding-left:0px;
    padding-right:0px
}


.propertyEven {
    background-color: #ffffff;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}

.propertyOdd {
    background-color: lightgrey;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}
```

EUQ Stylesheet

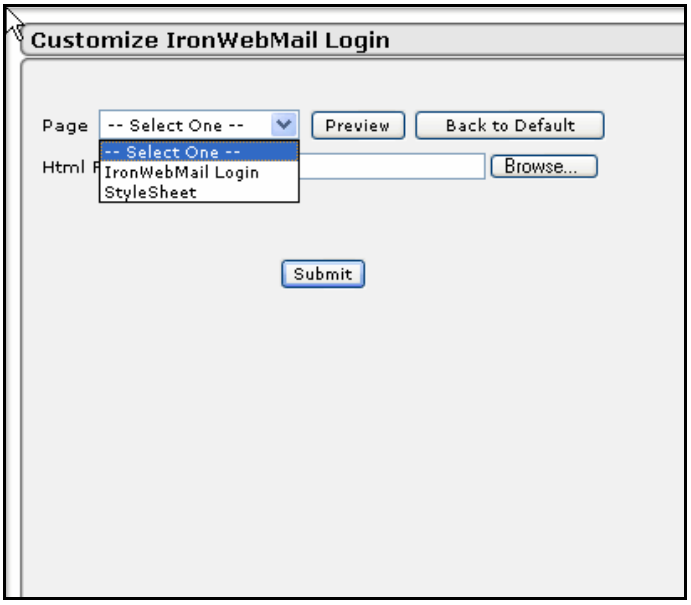
urq_customstyle[1].css

```
TD {
    font-family: verdana,helvetica,arial;
    font-size: 9px;
    color: black;
}

TH {
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    font-weight: bold;
    color: black;
    background-image : url('/images/thbackground.gif');
}

A {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}

A:visited {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}

A:hover {
  font: 10px verdana, sans-serif;
  color: #11568C;
  text-decoration: none;
}


BUTTON {
    font-family: verdana,helvetica,arial;
    font-weight: bold;
    font-size: 9px;
    color: black;
    padding-left:0px;
    padding-right:0px
}


.propertyEven {
    background-color: #ffffff;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}

.propertyOdd {
    background-color: lightgrey;
    font-family: verdana,helvetica,arial;
    font-size: 10px;
    border-width: 0px 0px 1px 0px;
    border-color: black;
    border-style: solid;
    line-height: 15px;
}
```

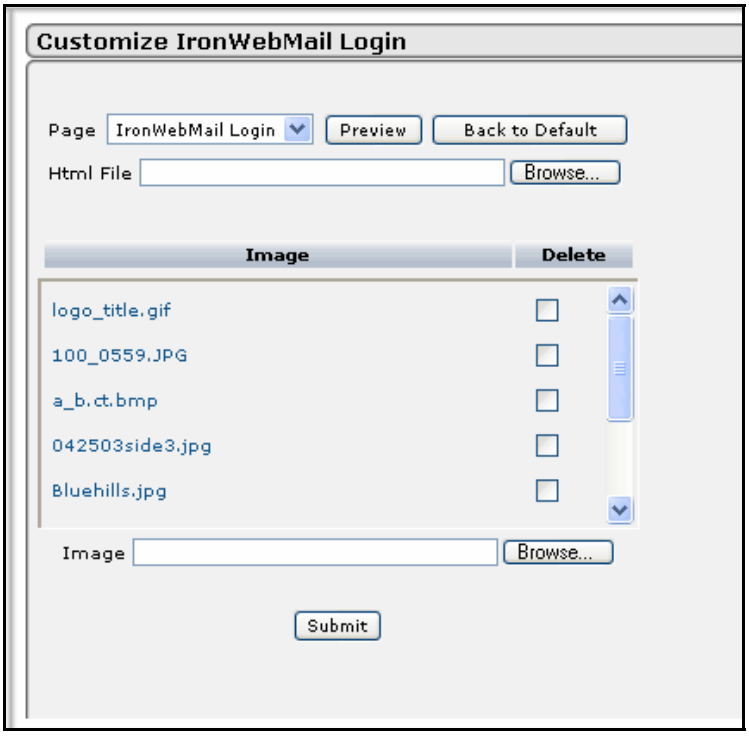
Performing Customizations

Each customizable page has its own stylesheet and its own default content, but customizing any of them follows the same general procedure. For the example that follows, assume the Administrator wants to customize the IronWebMail Login screen. The required steps are:

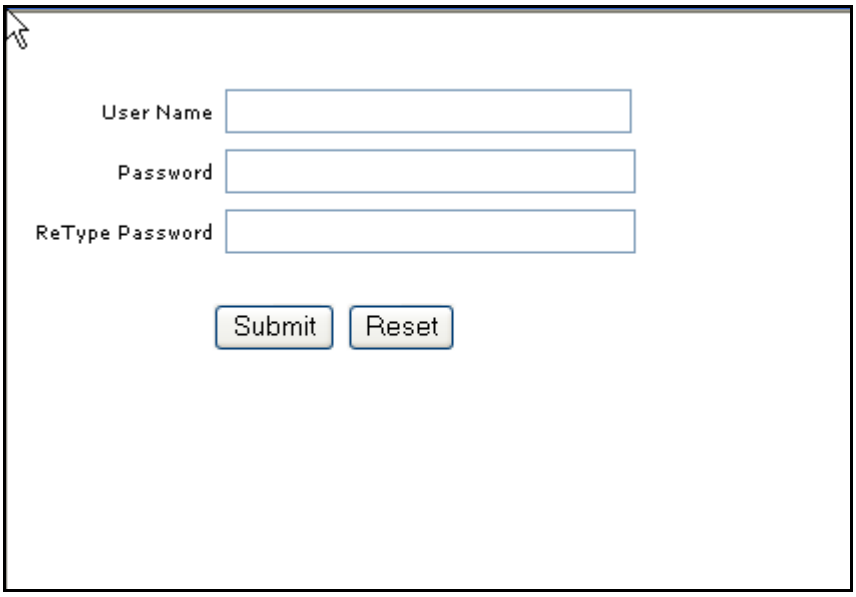
1. Navigate in IronMail to the customization screen (in this case, IWM Customized Login).



2. Select IronWebMail Login from the dropdown list; the screen will refresh to facilitate the customization. If any images have been downloaded for possible use, they will show in the table.



3. Click Preview. The default screen will display. This illustrates the default HTML template.



4. Open the template and modify it to create the changes desired. More information about modifying the template will be presented below.

   Note: you cannot have javascript present in the page itself. Modifications must be done separately.

5. Use the Browse button beside "HTML FIle" to select the modified template. Click **Submit**.
6. Click Preview to see what the HTML page will look like.
7. If images are required for the template, they must be prepended with the path */images/iwm/<image name>* so they will display in the previewer. The path is not required for the actual screen appearance.

Modifying the HTML Template

The customization of any of the pages for which changes are allowed requires modification of the HTML template for that page. The templates for the pages are maintained in the following files:

/ct/w3/admin/java/webapp/webadmin/swm_composemessage.html

/ct/w3/admin/java/webapp/webadmin/swm_maillist.html

/ct/w3/admin/java/webapp/webadmin/swm_login.html

/ct/w3/admin/java/webapp/webadmin/swm_viewmessage.html

/ct/w3/admin/java/webapp/webadmin/urq_maillist.html

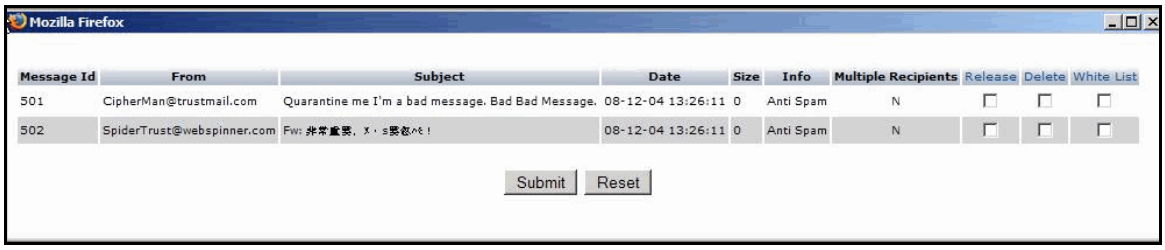
/ct/w3/admin/java/webapp/webadmin/iwm_login.html

An example using the EUQ Available Mail List is shown below.

The default template for the mail list displays all the columns:

```
<html>
<body>
<urq_maillist/>
</body>
</html>
```

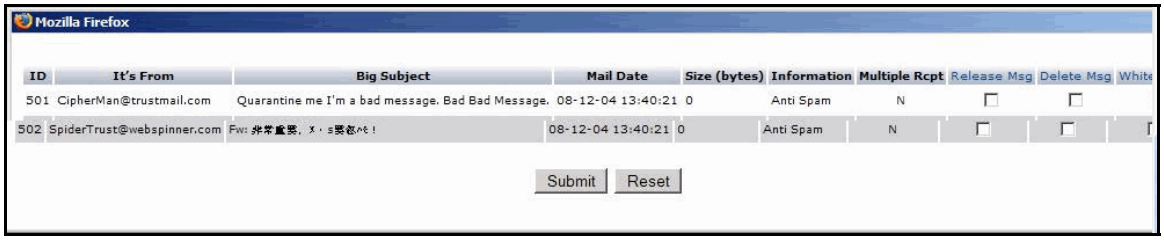
The preview of the screen as it is delivered looks like this:



The actual changes to be made to the screen are accomplished by modifying the urq_maillist tag. For example, if you want to show all the columns with different captions, the template might be modified to look like this:

```
<html>
<body>
<urq_maillist>
  <column key="id" value="ID" pos="1"/>
  <column key="from" value="It's From" pos="2"/>
  <column key="subject" value="Big Subject" pos="3"/>
  <column key="date" value="Mail Date" pos="4"/>
  <column key="size" value="Size (bytes)" pos="5"/>
  <column key="info" value="Information" pos="6"/>
  <column key="multircpt" value="Multiple Rcpt" pos="7"/>
  <column key="release" value="Release Msg" pos="8"/>
  <column key="delete" value="Delete Msg" pos="9"/>
  <column key="whitelist" value="WhiteList Msg" pos="10"/>
</urq_maillist>
</body>
</html>
```

The screen would now look like this:



APPENDICES

Appendix 1: Formatting Requirements for Importing Lists into IronMail version 4.5

PLEASE NOTE! IN ALL IMPORT FILES, ALL "|" (PIPE) CHARACTERS ARE REQUIRED, EVEN WHEN THEY ARE DELIMITING EMPTY OR OPTIONAL FIELDS.

Below are the various locations within the Web Administration interface where lists may be imported into IronMail 4.5:

1. **Mail Firewall > Allow Relay**

   The import file should contain one or more lines in the following format:

   ```
   IP_subnet|IP_sidenote
   ```

   Where **IP_subnet** is a 32-bit (four-octet) IP address or classful subnet. This value is required.

   Where **IP_sidenote** is any alphanumeric comment. This value is optional. The sidenote may contain simulated carriage returns if "<br>" is inserted at the desired location. Multiple “spaces” may be added to the sidenote by replacing the space with its HTML equivalent: " ".

   Some good examples of Allow Relay import file entries are:

   ```
   10.60.1|sample text
   1.2.3.4|
   1.2.11|first line of text<br>second line of text
   4.3.2|this       is text with extra
   spaces
   ```

   Some bad examples of Allow Relay import file entries are:

   ```
   xyz|xyz //the characters “xyz” are not a valid IP
   subnet
   10.65.1.111 //the pipe symbol ( | ) is missing
   ```

2. **Policy Manager > Queue Whitelist > Create**

   The import file should contain one or more lines in the following format:

```
type|direction|data|anti_spam_bypass|policy_manager_byp
ass|a
nti-virus_bypass
```

Where **type** is a required field and must contain one of the following values (without the quotation marks): "from domain", "to domain", "from email", "to email", or "ip address". (The names are case insensitive.) *Where* “direction” is a required field and must contain one of the following values (without the quotation marks): "inbound", "outbound", or "both". (The names are case insensitive.)

Where **data** is a required field and should contain valid domain, email, or IP address information. *Where* **anti_spam_bypass**, **policy_manager_bypass**, and **anti-virus_bypass** all have the format:

```
Feature:Sub-Feature
```

Where **Feature** is the numeric value of a Feature (see below)
Where **Sub-Feature** is the numeric value of a Sub-Feature (see below)

NOTE! At least one of the bypass definitions is required. Feature and Sub-Feature values can be given in any order. The colon is a required
delimiter between the Feature and Sub-Feature.

Allowed values:
Feature **7: Anti-Spam**:

Sub_features:
- 1 - Reverse DNS
- 2 - Realtime Blackhole List
- 3 - Statistical Lookup Service
- 5 - System Defined Header Analysis
- 6 - User Defined Header Analysis
- 9 - Enterprise Spam Profiler
- 10 - Bayesian Engine
- 11 - Sender Policy Framework

Feature **6: Policy Manager**:

Sub-Features:

1 - Mail Monitoring
2 - Encrypted Message Filtering
3 - Off Hour Delivery
4 - Attachment Filtering
5 - Content Filtering
6 - Message Stamping

Feature **5: Anti-Virus**:

Sub-Features:

1 - Sophos Engine
2 - McAfee Engine
3 - other engine?

Some good examples of whitelist entries in an import file are:

```
From
Domain|Inbound|foo.com|5:1,2|6:1,3,5|7:1,2,3,5
To Domain|Outbound|baz.com||6:1,3,5|7:1,2,3,5
From Domain|Both|bar.com|7:1,3,5|6:1,3|5:1
To Email|Both|abcd@foo.com||6:1,3,5|7:1,2,3,5
From Email|Both|abcd@foobaz.com|6:1,5|7:2,5|
IP Address|Outbound|12.13.12.13|||7:1,2
IP Address|Both|12.113.112.13|7:1||
```

3. Policy Manager > Group Manager > Definition

Import files for groups are a little different from others. The file may contain more than one group. Each group is defined on a single line of text. Thus, a single file may contain multiple “lists” of groups, with each group being defined in its line. A list of groups in an import file should contain one or more lines in the following format:

```
group_name|domain_based|data_list
```

Where **group_name** is a required field and is the name of the group

Where **domain_based** is a required field that accepts the following values: 0 = User-based Group 1 = Domain-based Group

Where **data_list** is a comma delimited list of domain names or email addresses (depending on the **domain_based** field value)

Some good examples of groups are:

```
group1|0|abc@ct.com,dbs@ct.com,snq@hotmail.com
group2|1|abc.com,cde.com,fgh.org
```

4. Attachment Filtering > Manage Rules > Extension Details List

Import files for attachment filtering should contain one or more lines in the format:

```
rule_name|file_ext_name|is_file|action|action_value|alter
nat
ive_action|alternative_action_value|quarantine_type|notif
ica
tion
```

Where **rule_name** is a required field and is an alpha string representing the "name of the rule" (e.g., "my blocked files").

Where **file_ext_name** is a required field and is an alpha string representing either a file *extension* or *filename*. The period (.) extension-delimiter is not allowed when entering an extension—user interface validation prohibits this string from beginning with a period.

Where **is_file** is a required field that accepts the following values:
0 = extension
1 = file

Where **action** is a required field and represents the exact name of Attachment Filtering Policy's actions (e.g., quarantine, copy, drop message)

Where **action_value** is a required field and represents the qualifying information related to the action (e.g., a **copy** action requires an email address as the **action_data**, and a **quarantine** action requires a number indicating how many days a message is to be quarantined)

Where **alternative_action** is a required field if the "action" field is "drop part" or "rename." For all other actions this field should be empty, represented by two pipe symbols with nothing inside them (||).

Where **alternative_action_value** is a required field if the "alternative_action" field is populated with data. This field may contain any action except "drop part" or "rename."

Where **quarantine_type** is a required field if the “action” field contains a **quarantine** action. This field must contain the exact name of an existing Quarantine Queue.

Where **notification** is a required field that accepts the following values:
0 = not enabled
1 = enabled

Some good examples of attachment filtering policies in an import file are:

```
blocked|exe|0|quarantine|0|||CFQ attachment filtering|1
allowed|pdf|0|Pass Through|||||0
dropped|*scr|1|Drop Part|Screensaver files are not
allowed this

     network.|Quarantine|0|CFQ screensavers|0
```

5. Content Filtering - Dictionaries - Edit

The import file should contain one or more lines in the following format:

```
word_or_phrase|weight|include
```

Where **word_or_phrase** is a required field and represents the alphanumeric string to search for.

Where **include** is a required field that accepts the following values:
0 = do not include
1 = include

Where **weight** is a required field and represents the weight of the word or phrase.include).

Some good examples of content filtering dictionary entries in an import file are:

0FFICE XP|100|1
200 medications|100|1

Appendix 2: Daily Policy Compliance Report - Summary and Statistics : 01/28/2004

Total Message Count
6807

Summary of Features:

Feature	Scanned	Detected	% Detected in Scanned	% Detected in Total
Anti-Virus	6816	334	4.90	4.91
Content Filtering	3540	0	0.00	0.00
Encrypted Message Filtering	5888	0	0.00	0.00
Attachment Filtering	5793	114	1.97	1.67
Mail Monitoring	3992	353	8.84	5.19
Anti-Spam	2620	622	23.74	9.14

Spam Summary:

Feature	Scanned	Detected	% Detected in Scanned	% Detected in Total Spam
User Defined Header Analysis	929	105	11.30	16.88
Statistical Lookup Service	940	449	47.77	72.19
System Defined Header	985	64	6.50	10.29

Analysis					
Realtime Blackhole List	980	142	14.49	22.83	
Enterprise Spam Profiler	983	0	0.00	0.00	
Reverse DNS	962	313	32.54	50.32	

Spam Action Counts:

Action	Enterprise Spam Profiler	Reverse DNS	Realtime Blackhole List	Statistical Lookup Service	User Defined Header Analysis	System Defined Header Analysis
Add Header	0	0	0	0	0	0
Log	0	126	0	0	8	0
Subject Rewrite	0	0	0	0	0	0
Quarantine	0	0	24	445	0	14
Secure Delivery	0	NA	NA	NA	0	NA
Forward	0	0	0	0	0	0
Copy	0	0	0	0	0	0
Drop Message	0	0	0	0	0	0

Feature Action Counts:

Action	Anti-Spam	Anti-Virus	Attachment Filtering	Content Filtering	Mail Monitoring	Encrypted Message

						Filtering
Reroute Message	NA	NA	0	0	188	NA
Forward as Attachment	NA	NA	0	0	0	NA
Add Header	0	NA	NA	NA	NA	NA
Pass Through	NA	NA	0	NA	NA	0
Log	134	NA	0	0	0	NA
Copy as Attachment	NA	NA	0	0	0	NA
Subject Rewrite	0	NA	0	NA	0	NA
Quarantine	483	0	0	0	70	0
Drop Part	NA	NA	0	0	NA	NA
Rename	NA	NA	0	NA	NA	NA
Replace	NA	NA	NA	0	NA	NA
Prefix	NA	NA	NA	0	NA	NA
Repackage	NA	336	NA	NA	NA	NA
Secure Delivery	0	NA	0	0	0	NA
Forward	0	NA	NA	NA	0	NA
Copy	0	NA	0	0	0	NA
Bypass File Encryption(Password Protection) Errors	NA	0	NA	NA	NA	NA
Drop Message	0	0	0	0	94	0

Top 20 *Policy Rules:*			
Rule **- Data**	**Message Count**	**% of Total**	

Mail Monitoring-Alert ERROR:	78	22.16 %	
Mail Monitoring-list.cr.yp.to	59	16.76 %	
Mail Monitoring-Daily Reports from	57	16.19 %	
Mail Monitoring-lawrence.hughes@ciphertrust.com	30	8.52 %	
Mail Monitoring-Banned Domains	19	5.40 %	
Mail Monitoring-Delivery Status Notification	19	5.40 %	
Mail Monitoring-Returned mail:	15	4.26 %	
Mail Monitoring-Undeliverable:	10	2.84 %	
Mail Monitoring-=?	7	1.99 %	
Mail Monitoring-failure notice	6	1.70 %	
Mail Monitoring-cash advance	4	1.14 %	
Mail Monitoring-stop smoking	4	1.14 %	
Mail Monitoring-Any Credit Accepted	4	1.14 %	
Mail Monitoring-lhughes@ciphertrust.com	3	0.85 %	
Mail Monitoring-cheap	3	0.85 %	
Mail Monitoring-Hot Req:	3	0.85 %	
Mail Monitoring-% OFF	3	0.85 %	
Mail Monitoring-save up to	3	0.85 %	
Mail Monitoring-out of the office	2	0.57 %	
Mail Monitoring-Last Chance to Register	2	0.57 %	
Mail Monitoring-auto loan	2	0.57 %	
Mail Monitoring-save upto	2	0.57 %	

Mail Monitoring-viagra	2	0.57 %
Mail Monitoring-valium	1	0.28 %
Mail Monitoring-burn fat while you sleep	1	0.28 %
Mail Monitoring-v1agra	1	0.28 %
Mail Monitoring-claim your	1	0.28 %
Mail Monitoring-Low Cost	1	0.28 %
Mail Monitoring-prescription medication	1	0.28 %
Mail Monitoring-Application Declined	1	0.28 %
Mail Monitoring-Banned Email Addresses	1	0.28 %
Mail Monitoring-italian-crafted rolex	1	0.28 %
Mail Monitoring-view photos of singles in your area	1	0.28 %
Mail Monitoring-home equity	1	0.28 %
Mail Monitoring-Delivery Failure:	1	0.28 %
Mail Monitoring-lose weight	1	0.28 %
Mail Monitoring-enter to win	1	0.28 %
Mail Monitoring-FREE shipping	1	0.28 %

Top 10 Policy Offenders:		
User Address	**Message Count**	**% of Total**
erroralert@ciphertrust.com	78	20.31 %
tim.thomas@ciphertrust.com	60	15.62 %

erroll.woods@ciphertrust.com	29	7.55 %
lawrence.hughes@ciphertrust.com	26	6.77 %
brians@ciphertrust.com	15	3.91 %
trent.greenwood@ciphertrust.com	11	2.86 %
troy.yeske@ciphertrust.com	9	2.34 %
david.scott@ciphertrust.com	8	2.08 %
penny.freeman@ciphertrust.com	7	1.82 %
sam.garcia@ciphertrust.com	7	1.82 %
bkavouras@ciphertrust.com	6	1.56 %

Top 10 Spammers:		
Sender	**Message Count**	**% of Total**
sneha.gokal@ciphertrust.com	19	2.74 %
teem@horizontal.letgo4u.com	15	2.16 %
mpeters@ciphertrust.com	14	2.02 %
coleen.leitch@ciphertrust.com	11	1.59 %
carl.thompson@ciphertrust.com	10	1.44 %
armando.rodriguez@ciphertrust.com	8	1.15 %
robert.babb@ciphertrust.com	7	1.01 %
ct_ops@sculptor.ciphertrust.net	7	1.01 %
jim.bockman@ciphertrust.com	7	1.01 %
joel.caracciolo@ciphertrust.com	6	0.86 %
steve.ganz@ciphertrust.com	6	0.86 %

savvynews@att.biz	6	0.86 %
adam.wosotowsky@ciphertrust.com	4	0.58 %
bill.erickson@ciphertrust.com	4	0.58 %
sc2003bb@eduexhibit.com	4	0.58 %
specials@123greetings.info	4	0.58 %
manthony@ciphertrust.com	3	0.43 %
michael.biscotti@ciphertrust.com	3	0.43 %
bounce-04af467e85@youdidto.com	3	0.43 %
keith.varnado@ciphertrust.com	3	0.43 %
moreinchescarriage@wildmail.com	3	0.43 %
ed.sherrouse@ciphertrust.com	3	0.43 %
navmse-mailmtl001@mei.ca	3	0.43 %
fool@foolsubs.com	3	0.43 %
nobody@cert.org	3	0.43 %

Top 10 Spam Recipients:		
Recipient	**Message Count**	**% of Total**
erroll.woods@ciphertrust.com	187	22.24 %
virusalerts@ciphertrust.com	41	4.88 %
david.scott@ciphertrust.com	29	3.45 %
ctmarketing@ciphertrust.com	19	2.26 %
bkavouras@ciphertrust.com	16	1.90 %
paul.judge@ciphertrust.com	15	1.78 %

david.scott@ciphertrust.com	14	1.66 %
dev_support@ciphertrust.com	12	1.43 %
sam.garcia@ciphertrust.com	11	1.31 %
sneha.gokal@ciphertrust.com	11	1.31 %
mwaldrop@ciphertrust.com	10	1.19 %
jeff.lake@ciphertrust.com	10	1.19 %
partnerprograms@ciphertrust.com	10	1.19 %

Top 10 Viruses:		
Virus Name	**Message Count**	**% of Total**
Sophos-W32/MyDoom-A	329	65.02 %
McAfee-W32/Mydoom@MM	91	17.98 %
McAfee-W32/Mydoom.a@MM	82	16.21 %
McAfee-W32/Bugbear.b@MM	1	0.20 %
Sophos-W32/Yaha-P	1	0.20 %
Sophos-SWEEP-ERROR	1	0.20 %
Sophos-W32/Bugbear-B	1	0.20 %

Appendix 3: Configuring IronWebMail for MS Exchange

Exchange 5.5 Configuration: The following outline presents the configuration that might be required on an Exchange 5.5 server:

1. Start the Internet Service Manager
    - Select Start->Programs->Windows NT 4.0 Option Pack-> Microsoft Internet Information Server->Internet Service Manager
    - The Microsoft Management Console should start.
2. Access the Properties screen for the Exchange Directory
    - Within the left directory tree frame, select Internet Information Server->Default Web Site->Exchange
    - Right click on the Exchange directory branch, then select the Properties option.
3. Configure the needed Exchange directory permissions
    - On the Exchange Properties window, select the Directory Security tab.
    - Click the Edit button under the Anonymous Access and Authentication Control section
    - Within the Authentication Methods window select two options:
        - Allow Anonymous Access
        - Basic Authentication
4. Access the Properties screen for the IISADMIN Directory
    - Within the left directory tree frame, select Internet Information Server->Default Web Site-> IISADMIN
    - Right click on the IISADMIN directory branch, then select the Properties option.
5. Configure the needed IISADMIN directory permissions
    - On the IISADMIN Properties window, select the Directory Security tab.
    - Click the Edit button under the Anonymous Access and Authentication Control section
    - Within the Authentication Methods window select one option:
        - Allow Anonymous Access

- **IronWebMail Configuration:**

0. Access the IronWebMail screen
1. Ensure the service is enabled and running
    - Click the Auto-Start icon (it should turn green)
    - Click the Running icon (it should turn green)
3. Click the IronWebMail link to access its properties window
4. Select the Portal Page from the “Select Routing Method” pull down, click the Submit button and then click the Close button to exit

5. Select the HTTP Routing link in the left navigation frame

6. Select the Portal Page submenu link

7. On the Portal Page screen, use the default HTTPS *protocol*. This will require end-users to use HTTPS to access the Portal Page

8. Enter any name in the Server Name column. This name will be used to identify a specific internal mail server on the Portal Page.

9. Enter the URL for the associated internal mail server followed by /exchange. Use https if the internal server has a valid server certificate and is properly configured; otherwise, use http (your selection will determine if the communication between IronMail and the internal mail server is secure (https) or unsecure (http). If the two servers (IronMail and the Internal Mail server) are not in the same building, then the customer should take the needed steps to use https.

Example: http://internalserver.test.com/exchange

Exchange 2000 Configuration: The following outline presents the configuration that might be required on an Exchange 2000 server:

1. Start the Internet Information Service Manager (IIS Mgr)
   - Select Start->Programs->Administrative Tools->IIS Mgr
   - The Internet Information Service Manager should be displayed.

2. Access the Properties screen for the Exchange Directory
   - Within the left directory tree frame, select the name of your Exchange 2000 server->Default Web Site->Exchange
   - Right click on the Exchange directory branch, and then select the Properties option.

3. Configure the needed Exchange directory permissions
   - On the Exchange Properties window, select the Directory Security tab.
   - Click the Edit button within the Anonymous Access and Authentication Control section.
   - Within the Authentication Methods window select one option:
     - Basic Authentication checkbox
   - Click the "OK" button to save your changes.
   - On the Directory Security tab, click the Edit button within the *IP Address* and *Domain Name* Restrictions window.
   - In the IP Address and Domain Name Restrictions window, select the "Grant Access" radio button. If needed, you can also click the "Add" button to enter any computer, group of computers or domains, which you want to deny OWA access. After all changes have been made, click the "OK" button on the IP Address and Domain Name Restrictions window to save your changes.
   - In the Exchange Properties window, click the "OK" button to close the window.

4. Access the Properties screen for the Exchweb Directory
   - Within the left directory tree frame, select the name of your Exchange 2000 server->Default Web Site-> Exchweb

- Right click on the Exchweb directory branch, and then select the Properties option.

5. Configure the needed Exchweb directory permissions
   - On the Exchweb Properties window, select the Directory Security tab.
   - Click the Edit button within the Anonymous Access and Authentication Control section.
   - Within the Authentication Methods window select one option:
     - Basic Authentication checkbox
   - Click the "OK" button to save your changes.
   - On the Directory Security tab, click the Edit button within the IP Address and Domain Name Restrictions window.
   - In the IP Address and Domain Name Restrictions window, select the "Grant Access" radio button. If needed, you can also click the "Add" button to enter any computer, group of computers or domains, which you want to deny OWA access. After all changes have been made, click the "OK" button on the IP Address and Domain Name Restrictions window to save your changes.
6. In the Exchweb Properties window, click the "OK" button to close the window.
7. Access the Properties screen for the IISAdmin Directory
   - Within the left directory tree frame, select the name of your Exchange 2000 server->Default Web Site-> IISAdmin
   - Right click on the IISAdmin directory branch, and then select the Properties option.
8. Configure the needed IISAdmin directory permissions
   - On the IISAdmin Properties window, select the Directory Security tab.
   - Click the Edit button under the Anonymous Access and Authentication Control section
   - Within the Authentication Methods window select TWO options:
     - Basic authentication checkbox and
     - Integrated Windows authentication checkbox
   - Click the "OK" button to save your changes.
   - On the Directory Security tab, click the Edit button within the IP Address and Domain Name Restrictions window.
   - In the IP Address and Domain Name Restrictions window, select the "Grant Access" radio button. If needed, you can also click the "Add" button to enter any computer, group of computers or domains, which you want to deny OWA access. After all changes have been made, click the "OK" button on the IP Address and Domain Name Restrictions window to save your changes
9. Access page 3 of the "XWEB: Troubleshooting HTTP 401.x Errors in Outlook Web Access" document and ensure the Exchange 2000 administrator has added the necessary access rights for:
   - Log on Locally access

- Access This Computer From the *Network* access (essential for remote access)

10. After all changes have been made, the Exchange 2000 administrator should stop and restart the Exchange 2000 server. It would be sufficient to stop and restart the IIS Manager, but there are so many services, which depend on the IIS Manager that it is easier to restart the server.

- **IronWebMail Configuration:**

0. Access the IronWebMail screen

1. Ensure the service is enabled and running
   - Click the Auto-Start icon (it should turn green)
   - Click the Running icon (it should turn green)

3. Click the IronWebMail link to access its properties window

4. Select the Portal Page from the "Select Routing Method" pull down, click the Submit button and then click the Close button to exit.

5. Select the HTTP Routing link in the left navigation frame

6. Select the Portal Page submenu link

7. On the Portal Page screen, use the default HTTPS protocol. This will require end-users to use HTTPS to access the Portal Page

8. Enter any name in the Server Name column. This name will be used to identify a specific internal mail server on the Portal Page.
   - Enter the URL for the associated internal mail server followed by /exchange. Use https if the internal server has a valid server certificate and is properly configured; otherwise, use http (you selection will determine if the communication between IronMail and the internal mail server is secure (https) or insecure (http). For the server name, use it fully-qualified name rather than its IP address. The IP address will work, but it will require that the end user enter their login credentials twice. If the two servers (IronMail and the Internal Mail server) are not in the same building, then the customer should take the needed steps to use https.
   - Example: http://mail.ex.ctqa.net/exchange

Appendix 4: What is LDAP?

Simply put, LDAP is an internet *protocol* that email programs use to look up contact information from a server.

Printed directories, alphabetical or classified lists of resources containing names, location, identifying information, etc., are important tools in providing library services. The purpose of electronic directories is not much different from that of printed directories. They provide information like names, addresses, locations and other information about people and organizations. In a LAN or WAN, this information can also be used for e-mail addressing, user authentication or network security, among other things. Directories are essential for effectively navigating the Web.

Early directories were proprietary, but the need for an open standard soon arose, resulting in the definition of X.500. This standard has found resistance in being adopted, however, because the resulting Directory Access Protocol (DAP) is too complex to implement easily and too large to run on desktop PC's.

That's where LDAP comes in. Lightweight Directory Access Protocol (LDAP) enables corporate directory entries to be arranged in a hierarchical structure reflecting geographic and organizational boundaries. While it lacks some of X.500's power, LDAP makes up for it in four ways:

- LDAP is designed to run over TCP, so it is ideal for internet and intranet applications;
- LDAP has simpler functions so it is easier and less expensive to implement;
- LDAP encodes the protocol elements in a less complex way, making it easier to code and decode requests; and,
- LDAP servers make referrals, much like a librarian telling you, "What you want is across town." LDAP servers return only results or errors.

LDAP Directories

Anytime you hear the words "computer," "managing," and "information" in the same sentence, you immediately know a database is involved. Directories are specialized databases that keep track of information distributed on a network. The major characteristics of LDAP directories are:

- Platform independence, allowing cross-platform access to data by any LDAP-aware application;
- Relatively static data that is seldom modified;
- Extremely fast read operations, so tuned because the data is read frequently but changed rarely;
- Distributable, meaning the data can be located on a number of systems on the network for redundancy, performance, and scalability;
- Hierarchical, to ensure there is an authoritative source of the data;
- Relatively secure, allowing secure delegation of read and modification authority based on needs, using ACIs(Access Control Interfaces);
- Object-oriented;
- Standards-based, using a standard schema, available to all applications that use the directory;
- Capable of accepting multi-value or single-value attributes; and,
- Capable of multi-master replication, providing self-healing directories.

LDAP Storage

LDAP servers are generally optimized for read-intensive operations, but are not well suited for storing data where changes are frequent. A decision to use and LDAP directory can be based on affirmative answers to the following questions:

- Should the data be available across platforms?
- Does the data need to be accessible from a number of computers or applications?
- Do the records to be stored change a few times per day or less?
- Does it make sense to store the data in a flat database instead of a relational database?

As a *rule*, if you can imagine storing the data on a big electronic Rolodex, you can easily store it on and LDAP directory.

Appendix 5: Tips and Guidelines

This section lists some helpful information for using IronMail.

Special Characters in Email Addresses

The email address you enter to apply rules to a single individual can contain any letter or number, plus certain special characters. Allowable characters are shown below:

!	#	$	%
&	'	*	+
-	/	=	?
^	_	`	{
|	}	~	

File Types From Which IronMail Can Extract Content

The file types listed below can be processed by IronMail's Content Extraction Queue. The extracted content is used by processes in SuperQueue, such as Attachment Filtering.

File Extensions

123	doc	mpp	pqf	sam	wp
as	htm	nfo	pre	txt	xlc
aw	jtd	pcw	prz	utx	xls
bh2	lwp	pdf	rft	wb3	xy
csv	mmf	ppt	rtf	wks	zip

Appendix 6: Vulnerability Assessment Report

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which where alive and responding during test	1
Number of security holes found	3
Number of security warnings found	10

Host List	
Host(s)	**Possible Issue**
10.50.40.30	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
10.50.40.30	netbios-ssn (139/tcp)	Security hole found
10.50.40.30	loc-srv (135/tcp)	Security warning(s) found
10.50.40.30	microsoft-ds (445/tcp)	Security notes found
10.50.40.30	blackjack (1025/tcp)	Security notes found
10.50.40.30	ms-sql-s (1433/tcp)	Security hole found
10.50.40.30	commplex-main (5000/tcp)	Security warning(s) found
10.50.40.30	general/tcp	Security warning(s) found
10.50.40.30	ms-sql-m (1434/udp)	Security hole found
10.50.40.30	general/udp	Security notes found
10.50.40.30	ntp (123/udp)	Security warning(s) found
10.50.40.30	general/icmp	Security warning(s) found
10.50.40.30	netbios-ns (137/udp)	Security warning(s) found

Security Issues and Fixes: 10.50.40.30		
Type	**Port**	**Issue and Fix**
Vulnerability	netbios-ssn (139/tcp)	. It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$ Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html . All the smb tests will be done as "/" in domain CIPHERTRUST CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222 Nessus ID : 10394
Warning	netbios-ssn (139/tcp)	The domain SID can be obtained remotely. Its value is : CIPHERTRUST : 5-21-533428487-1518886676-1846952604 An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445 Risk factor : Low CVE : CVE-2000-1200 BID : 959 Nessus ID : 10398
Warning	netbios-ssn (139/tcp)	The host SID can be obtained remotely. Its value is : CTWW148 : 5-21--1359260937-153307058--1928471394 An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445 Risk factor : Low CVE : CVE-2000-1200 BID : 959 Nessus ID : 10859
Informational	netbios-ssn (139/tcp)	The remote native lan manager is : Windows 2000 LAN Manager The remote Operating System is : Windows 5.1 The remote SMB Domain Name is : CIPHERTRUST Nessus ID : 10785
Warning	loc-srv (135/tcp)	DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low Nessus ID : 10736
Informational	microsoft-ds (445/tcp)	A CIFS server is running on this port Nessus ID : 11011

Informational	blackjack (1025/tcp)	Here is the list of DCE services running on this port: UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1 Endpoint: ncacn_ip_tcp:10.50.40.30[1025] UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1 Endpoint: ncacn_ip_tcp:10.50.40.30[1025] UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1 Endpoint: ncacn_ip_tcp:10.50.40.30[1025] Nessus ID : 10736
Vulnerability	ms-sql-s (1433/tcp)	The remote MS SQL server is vulnerable to the Hello overflow. An attacker may use this flaw to execute commands against the remote host as LOCAL/SYSTEM, as well as read your database content. Solution : Install Microsoft Patch Q316333 at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&sd=tech or disable the Microsoft SQL Server service or use a firewall to protect the MS SQL port (1433). Risk factor : High CVE : CAN-2002-1123 BID : 5411 Nessus ID : 11067
Informational	ms-sql-s (1433/tcp)	Microsoft SQL server is running on this port. You should never let any unauthorized users establish connections to this service. Solution: Block this port from outside communication Risk factor : Medium CVE : CAN-1999-0652 Nessus ID : 10144
Informational	ms-sql-s (1433/tcp)	Microsoft SQL server is running on this port. You should never let any unauthorized users establish connections to this service. Solution: Block this port from outside communication Risk factor : Medium CVE : CAN-1999-0652 Nessus ID : 10144

Warning	commplex-main (5000/tcp)	The remote host is running Microsoft UPnP TCP helper. If the tested network is not a home network, you should disable this service. Solution : Delete the registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\SSDPSRV and reboot the remote host Risk Factor : Low Nessus ID : 11765
Informational	commplex-main (5000/tcp)	A web server is running on this port Nessus ID : 10330
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Warning	general/tcp	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low Nessus ID : 10201
Vulnerability	ms-sql-m (1434/udp)	The remote host MS SQL server is vulnerable to several overflows which could be exploited by an attacker to gain SYSTEM access on that host. Note that a worm is exploiting this vulnerability in the wild. Solution : See MS Advisory MS02-061 Risk factor : High CVE : CAN-2002-1137, CAN-2002-1138, CAN-2002-0649, CVE-2002-0650, CAN-2002-1145, CAN-2002-0644, CAN-2002-0645, CAN-2002-0721 BID : 5310, 5311 Nessus ID : 11214

Warning	ms-sql-m (1434/udp)	Here is the reply to a MS SQL 'ping' request : ServerName;CTWW148;InstanceName;MSSQLSERVER;IsClustered;No;Version;8.00.194;tcp;1433;np;\\CTWW148\pipe\\sql\query;; *** Note that the version number might be inaccurate, as Microsoft *** decided to not increase it with new releases of its software It is suggested you filter incoming traffic to this port Nessus ID : 10674
Informational	general/udp	For your information, here is the traceroute to 10.50.40.30 : 10.50.1.1 10.50.40.30 Nessus ID : 10287
Warning	ntp (123/udp)	An NTP server is running on the remote host. Make sure that you are running the latest version of your NTP server, has some versions have been found out to be vulnerable to buffer overflows. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. If you happen to be vulnerable : upgrade Solution : Upgrade Risk factor : High CVE : CVE-2001-0414 BID : 2540 Nessus ID : 10647
Informational	ntp (123/udp)	It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings. Theoretically one could work out the NTP peer relationships and track back network settings from this. Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore Risk factor : Low Nessus ID : 10884
Warning	general/icmp	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524 Nessus ID : 10114

Warning	netbios-ns (137/udp)	. The following 6 NetBIOS names have been gathered : CTWW148 CIPHERTRUST CTWW148 CTWW148 CIPHERTRUST JFRANCIS . The remote host has the following MAC address on its adapter : 0x00 0x08 0x74 0xc4 0x0d 0xcb If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621 Nessus ID : 10150

This file was generated by Nessus, the open-sourced security scanner.

Document History:

Date	Comment	Author
07/15/2004	Began new version of IronMail User Guide (version 4.5) using version 4.1 plus design documents as a basis.	J. Francis
9/30/2004	Completed Beta Version of the 4.5 User Guide	J. Francis
10/22/2004	Completed Final Draft of the 4.5 User Guide	J. Francis
10/28/2004	Added Connection Management to produce User Guide for IronMail 4.5, SR 1.	J. Francis
11/03/2004	Final cleanup and formatting.	J. Francis

INDEX

A

Action Codes 427
Add Domain Routing..... 42
Adding ESP Policies 283
Adding Lists 157
Address Masquerade..... 113
ADE Rules 69
Alert Class 383
Alert Levels 382
Alert Manager 382
Alert Mechanism 388
Alert Viewer 392
Alerts 378
Allow Relay 37
Allowed IPs 468
Analysis Console 56
Anomaly Detection 63
Anti-Spam Overview..... 231
Anti-Spam Queue Detailed Log 445
Anti-Virus 222
Anti-Virus File Updating
  Log File 230
Anti-Virus File Updating 230
Apply Attachment Filtering Rules 159
Apply Content Filtering Rules 182
Apply Encrypted Message Rules..... 141
Apply ESP Rules 282
Apply Mail Monitor Rules 129
Archive..... 461
Attachment Filtering.....148, 157, 165
Auto Anti-Virus Updates..... 227

B

Backup 482
Bayesian 274
Bayesian Engine..... 271
Bayesian Training Scenarios 273
Best Content Filtering Practices..... 190
Boundary
  Boundary..... 351
Boundary..... 351
Browser Issues 471

C

Cascading Stylesheets 537
Certificate Manager 338
Certificate Types 341
Change Password 471
Check Tool 487
Checking Logs 371
CipherTrust Experience..... 287
Cleanup Schedule..... 463
CMC 13
Command Line Interface 503
Command Overview..... 503
Configuration..... 473
Configure
  EUQ Web Page 205
Configure 205
Configure 470
Configure Analysis Console 58
Configure Anomaly Detection 63
Configure Anti-Virus 222
Configure Auto-Updates..... 497
Configure End User Quarantine 202
Configure EUQ Whitelists..... 218
Configure Mail Certificates..... 465
Configure Mail-VPN..... 47
Configure Queues 301
Configure Router..... 363
Configure Secure Web Delivery..... 363
Configure Server 365
Configuring ESP 277
Configuring IronMail 13
Configuring IWM
  MS Exchange 559
Configuring IWM..... 559
Configuring Mail Certificates..... 350
Configuring Mail Services 24
Connection Control 70
Consolidated Quarantine Server..... 336
Consolidating Notifications 214
Content Extraction 165
Content Filtering..... 189
Content Filtering Queue Detailed Log..... 446
Controlling
  Gateway..... 21
Controlling 21
Create Anomaly Rules 65
Create Whitelists..... 104
Creating IronMail Policy 104
CSV File
  Understanding..... 423
CSV File..... 423
CSV Reports..... 420
Current Anti-Virus Information..... 225
Current Messages 309
Custom IWM Page 89
Customizable Pages 529
Customizing EUQ..... 536
Customizing IronMail Pages 529

Customizing IWM 534
Customizing SWD..... 529
Customizing SWD Pages 370

D

Daily Policy Compliance Report 551
Dangerous Extensions..... 166
Dashboard 525
Date..... 489
Default Replacement Text 167
Definition 117
Denial
Service Protection 53
Denial 53
Deny Lists 234
Dictionaries 169
DNS Configuration..... 16
DNS Hijack Protection 379
Documentation
History 573
Documentation 573
Domain ESP Policies 286
Domain_Priority 330
Domain-based Routing..... 39
Dropped Email Alerts..... 411

E

EDIT Command..... 505
Edit Domain Routing 41
Editing ESP Policies..... 285
Encrypted Message Filtering..... 135
End User Quarantine Release 201
End User Quarantine User List..... 206
Enterprise Spam Profiler 274
Enterprise Spam Reporting..... 291
ESP ...189, 240, 246, 251, 263, 269, 271, 274
ESP Profile..... 275
EUQ Mailing List..... 209
EUQ Process Overview 202
EUQ Web Page
Configure..... 205
EUQ Web Page..... 205
EUQ Whitelisting..... 215
Examining Connections..... 23
Examining Messages..... 93
Export 345
Extension Over-ride 223
External S/MIME 354

F

Filesystem Integrity 62

G

Gateway
Controlling 21
Gateway..... 21
Gateway Security 21
Gateway Threats 21
Generate CSR..... 338
Group 286
Group Manager..... 115
Guidelines..... 565

H

Header Analysis Filters..... 257
Health Monitor 373
Health Monitor Tests..... 378
HELP Command 505
History
Documentation 573
History..... 573
Host-Based Routing 77
HTTP Routing..... 76

I

IMAP4..... 49
Import Formats
Importing Lists 545
Import Formats..... 545
Importing Lists
Import Formats..... 545
Importing Lists 545
Importing MIBs 412
Initial Configuration 4
Inside
SuperQueue 98
Inside..... 98
Install Certificate 342
Installing PGP Public Keys 91
Internal Mail Server Configuration 16
Internal PGP 360
Internal Routing 46
Internal S/MIME 357
Introducing 93
IronMail..... 1, 473
IronMail Security Strategy..... 338
IronMail-generated Alerts
Table..... 394
IronMail-generated Alerts..... 394

L

LDAP..... 115, 563
LDAP-based Routing 42

Level Protection 51
License Manager 498
Local Deny List 234
Log File
  Anti-Virus File Updating 230
Log File 230
Log File 412
Log Level Warning 51
Log Levels 438

M

Mail Monitor 121
Mail Notification 198
Mail Routing 39
Mail-Firewall 23
Mail-IDS 51
Mail-IDS Updates 496
Maintaining EUQ Whitelists 216
Manage Attachment Filtering Rules 150
Manage Message Stamping Rules 191
Manual Anti-Virus Updates 228
Message Stamping 191
Messages
  Searching 315
Messages 315
Monitoring 373
Monitoring Conditions 517
MS Exchange
  Configuring IWM 559
MS Exchange 559
Multiple Blacklists 245

N

Network Firewall Configuration 17
Network Level Protection 56

O

Off-Hour Delivery 146
Opening Graphs 517
Outbound Queue 309
Out-of-Band Management 476
Overview 337

P

Password Cracking 54
Password Strength 55
Path-Based Routing 80
Performing Customizations 541
PGP 358
Policy Manager 103
POP3 Services 49
Port 465 32
Portal Login Page 86
Portal Page Routing 83
Power Down 489
Preliminary Information 3
Process ID Numbers 454
Program Integrity 62
Protection 62

Q

QChannel 102
QServer 100
QSpinner 101
Quarantine Queue
  Using 335
Quarantine Queue 335
Quarantine Release Notification 210
Quarantine Types 333
Quarantined Messages 313
Queue Graphs 519
Queue Information Data
  Refreshing 335
Queue Information Data 335
Queue Whitelist 104

R

RBL 246
RBL Deny List 236
RDNS 240
Realtime Blackhole List 241
Refreshing
  Queue Information Data 335
Refreshing 335
Regular Expression Header Analysis 252
Reporting Utilization 517
Reports 373, 412
Resetting Keys 501
Restart 489
Restore 485
Reverse DNS Deny List 237
Reverse_DNS 238
RFC821 versus RFC822 Headers 263
Routing 478
RUN Command 506

S

S/MIME 354
SDHA 263
Search Whitelists 107
Searching
  Messages 315
Searching 315

Searching Current Messages 317
Searching Processed Messages 327
Searching Quarantined Messages 321
Secure Delivery 350
Secure Web Delivery Server 363
Secure WebMail 73
Sender Policy Framework Lookup 269
Serial Port 479
Service Protection
  Denial 53
Service Protection 53
SET Command 507
Setting Up IronMail 3
Show Anomaly Rules 68
SHOW Command 509
Signature Configuration 89
Signature Manager 60
Signature Updates 61
SLS 251
SLS Bypass 251
SMTPIS Service 32
SMTPProxy Detailed Log#MessageID 448
Software Updates 491
Spam Order 287
Spam Summary Report 420
SPF 271
Spoofed Message Protection 32
SSH Configuration 480
SSL 351
Statistical Lookup Service 247
Statistics 551
Store CMC Key 499
Storing Certificates 343
Strong Client Authentication 90
Summary 551
Summary Logs 450
SuperQueue
  Inside 98
SuperQueue 98
SuperQueue Flow 100
SWD Overview 362
SysLog Configuration 438
SYSTEM Command 514
System Defined Header Analysis 252
System Graphs 521
System Level 62

T

Table
  IronMail-generated Alerts 394
Table 394
TAIL Command 515
TEST Command 515
Threat Response Updates 495
Time 489
Tips 565
Trusted Source 246

U

UDHA 269
Understanding
  CSV File 423
Understanding 423
Understanding Detailed Logs 445
UPS Statistics 488
URL Decoding 175
URL Filtering 174
User 286
User Accounts 466
User Defined Header Analysis 263
User List 366
User Spam Reporting 288
User Tip 330
Using
  Quarantine Queue 335
Using 335

V

View Whitelists 109
Virus Updates 493
Vulnerability Assessment 71
Vulnerability Assessment Report 567

W

Whitelist Rules 109